A Conceptual Framework for the Regulation of Cryptocurrencies

Omri Marian†

INTRODUCTION

This Essay proposes a conceptual framework for the regulation of transactions involving cryptocurrencies. Cryptocurrencies offer tremendous opportunities for innovation and development but are also uniquely suited to facilitate illicit behavior. The regulatory framework suggested herein is intended to support (or at least not impair) cryptocurrencies' innovative potential. At the same time, it aims to disrupt cryptocurrencies' criminal utility. To achieve these purposes, this Essay proposes a regulatory framework that imposes costs on the characteristics of cryptocurrencies that make them especially useful for criminal behavior (in particular, anonymity) but does not impose costs on characteristics that are at the core of cryptocurrencies' generative potential (in particular, the decentralization of value-transfer processes). Using a basic utility model of criminal behavior as a benchmark,[1] this Essay explains how regulatory instruments can be so designed. One such regulatory instrument is proposed as an example—an elective anonymity tax on cryptocurrency transactions in which at least one party is not anonymous.

There has been increasing interest in the regulation of cryptocurrencies, with many inquiries focusing on the regulation of cryptocurrencies within discrete areas of law.[2] This Essay

† Assistant Professor of Law, University of Florida Levin College of Law. For helpful comments and critique I thank Professors Michael Abramowicz, Andrew Hayashi, Danny Sokol, as well as Sarah Meiklejohn and participants at the ABA Tax Section's 2-14 Joint Fall CLE Meeting and the 9th Annual Junior Tax Scholars Workshop.

1 See note 30 and accompanying text.

2 See generally, for example, Stephen T. Middlebrook and Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 Wm Mitchell L Rev 813 (2014); Jerry Brito, Houman B. Shadab, and Andrea Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 Colum Sci & Tech L Rev (forthcoming 2014), online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423461 (visited Nov 26, 2014); Nicholas A. Plassaras, *Regulating Digital Currencies: Bringing Bitcoin within the Reach*

contributes to the discussion by suggesting a generic framework for the design of regulatory instruments that address cryptocurrencies. The suggested framework is both direct and indirect in its approach. It directly addresses possible incentives to use cryptocurrencies illicitly. Indirectly, the framework takes advantage of the unique structure of cryptocurrencies' protocols by making legitimate users passive agents of regulatory efforts. Specifically, a derivative benefit of the suggested framework is that the legitimate use of cryptocurrency would have the effect of making cryptocurrencies systemically less suitable for illicit use.

This Essay is structured as follows: Part I briefly discusses the core innovation of cryptocurrencies—the public ledger—and explains its positive potential as well as the challenges that it presents to traditional regulatory models. Part II introduces the proposed regulatory approach in the abstract, using a basic utility model of criminal behavior as a linchpin for discussion. Part III describes an elective tax on anonymity to demonstrate how the suggested framework might operate in the context of tax evasion. Part IV discusses possible critiques of the suggested approach. The Essay concludes with a call for further discussion of this new regulatory area.

I. VIRTUES, VICES, AND REGULATORY CHALLENGES

Bitcoin, a cryptocurrency[3] that is best known as a peer-to-peer electronic cash system, is touted as being as revolutionary as the Internet.[4] The potential of Bitcoin[5] and other

of the IMF, 14 Chi J Intl L 377 (2013). For two recent exceptions to the field-tailored approach that advocate a broader view of the problem, see Andy Yee, *Internet Architecture and the Layers Principle: A Conceptual Framework for Regulating Bitcoin*, 3 Internet Pol Rev 1, 6–7 (2014); Kevin V. Tu and Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 Wash L Rev (forthcoming 2015), online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2485550 (visited Nov 16, 2014).

[3] I use the term "cryptocurrency" to refer to any digital currency that relies on peer-to-peer cryptography for the validation of value transfers.

[4] See, for example, Bloomberg TV, *Here's How Bitcoin Is Like the Early '90s Internet* (Mar 28, 2014), online at http://www.bloomberg.com/video/here-s-how-bitcoin-is-like-early-90-s-internet-dU0H7ADwTl6arrq122kHPg.html (visited Nov 16, 2014); Saumya Vaishampayan, *Bitcoin Is Like the Early Internet, Minus the VC Money*, Market Extra (MarketWatch Apr 28, 2014), online at http://www.marketwatch.com/story/bitcoin-venture-capital-money-hasnt-kept-up-with-buzz-2014-04-28 (visited Nov 16, 2014).

[5] The term "Bitcoin" is commonly used to refer to the technology, as opposed to "bitcoin," which refers to the virtual currency that is based on the technology and represents one possible application of it. See Kate Cox, *Bitcoin: What the Heck Is It, and How Does It Work?*, Consumerist (Mar 4, 2014), online at

cryptocurrencies extends beyond their applications as units of account or mediums of exchange. Rather, the unique technological innovation common to most cryptocurrencies is a public ledger that functions as a decentralized system for recording ownership and value transfers. While the technical operation of the ledger is complex,[6] the core idea is rather simple. When an owner of a cryptocurrency (which can be described as an electronic token) transfers the cryptocurrency to a recipient, the transaction is verified in a process called "mining." A crowd of "miners" consults the ledger, verifies the owner's claim of ownership, and documents the transfer to the recipient, who from now on is logged on the ledger as the owner of the cryptocurrency. The verification process is a competitive one. The miners do not simply verify the transaction; they compete to solve a complex cryptographic problem. The first miner to succeed wins the competition, logs the transaction on the ledger, and is awarded a new batch of cryptocurrencies. The new batch of cryptocurrencies is automatically generated by the software and functions both as an incentive to participate in the mining process[7] and as a decentralized mechanism for the issuance of new cryptocurrencies. Anyone can become a miner by downloading the necessary software. Cryptocurrency software is open-source and generally not controlled by a central entity.[8]

To summarize, cryptocurrencies are essentially protocols that allow for the validation of transactions without the need for a trusted third party such as a bank, credit card company, escrow agent, or recording agency.[9] As such, cryptocurrencies hold great innovative potential. They have been described as a "generative" technology on which powerful applications can be built.[10] For example, cryptocurrencies may dramatically reduce

---

http://consumerist.com/2014/03/04/bitcoin-what-the-heck-is-it-and-how-does-it-work (visited Nov 16, 2014).

6 For a thorough explanation of the verification process, see Ritchie S. King, Sam Williams, and David Yanofsky, *By Reading This Article, You're Mining Bitcoins*, Quartz (Dec 17, 2013), online at http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins (visited Nov 16, 2014).

7 In the alternative, miners could charge a fee for verifying the transaction.

8 See King, Williams, and Yanofsky, *By Reading This Article, You're Mining Bitcoins* (cited in note 6).

9 Brito, Shadab, and Castillo, 16 Colum Sci & Tech L Rev at *5 (cited in note 2).

10 The term "generative" is used here in the sense suggested by Jonathan Zittrain, who describes generativity as "a function of a technology's capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery, and accessibility." Jonathan L. Zittrain, *The Generative Internet*, 119 Harv L Rev 1975, 1981 (2006). For a reference to Bitcoin as a "generative" technology, see, for example, Timothy B. Lee,

transaction costs associated with value transfers,[11] engender access to financial transactions within sectors of the population that do not have access to traditional financial institutions,[12] avoid the pitfalls of managed or commodity-based monetary systems,[13] and allow for the creation of self-enforcing smart contracts that do not rely on financial institutions, lawyers, or accountants for their execution.[14]

However, cryptocurrencies are also uniquely suited to facilitate harmful behaviors for two reasons.[15] First, the only truly public feature of the ledger is the documentation of ownership and transfers. The owners themselves are not identified by name on the ledger, but rather by a set of letters and numbers representing their public cryptocurrency address (which, together with the private key that proves ownership of that address, constitute the owner's cryptocurrency "wallet").[16] Anyone can freely create as many wallets as he or she desires, at practically zero cost, without providing any identifying information.[17] This relatively high level of anonymity makes it difficult for regulators to identify individuals who use the protocol for illicit value transfers.

Here's What Critics Miss about Bitcoin's Long-Term Potential, The Switch (Wash Post Dec 3, 2013), online at http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/03/heres-what-critics-miss-about-bitcoins-long-term-potential (visited Nov 16, 2014).

[11] See Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* 10 (Mercatus 2013).

[12] See id at 14–15 (discussing how bitcoin can improve financial access as a means to fight poverty).

[13] See George Selgin, *Synthetic Commodity Money* *11 (University of Georgia Working Paper, Apr 2013), online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118 (visited Nov 16, 2014).

[14] Brito and Castillo, *Bitcoin* at 16 (cited in note 11); Vitalik Buterin, *DAOs Are Not Scary, Part 1: Self-Enforcing Contracts and Factum Law*, Bitcoin Magazine (Feb 24, 2014), online at http://bitcoinmagazine.com/10468/daos-scary-part-1-self-enforcing-contracts-factum-law (visited Nov 16, 2014).

[15] A recent report by the Europol, for example, suggests that cryptocurrencies "are heavily abused by criminals." Europol, *The Internet Organised Crime Threat Assessment (iOCTA)* *42 (2014), online at https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf (visited Nov 16, 2014).

[16] See Bitcoin, *Some Bitcoin Words You Might Hear*, online at https://bitcoin.org/en/vocabulary#private-key (visited Nov 20, 2014).

[17] See Omri Marian, *Are Cryptocurrencies* Super *Tax Havens?*, 112 Mich L Rev First Impressions 38, 42 (2013).

It should be noted, however, that most cryptocurrencies are not completely anonymous, but rather are pseudonymous.[18] For example, if the identity of some wallet owners is known, it is theoretically possible to use these known nodes in the system to build a "transaction graph" that tracks each particular cryptocurrency. By doing so, one could expose the identity of owners of unknown wallets with which the known wallets transacted.[19] However, this technique requires complex analysis and concentrated effort that may be worthwhile only when a particular wallet is suspected of engaging in illicit activity.

The second reason that cryptocurrencies are suited for criminal activity is that our financial-regulation system heavily relies on regulating intermediaries that are uniquely positioned to disrupt misconduct. For example, we subject financial institutions to "know-your-costumer rules" in order to prevent money laundering, use banks as tax-withholding agents to prevent tax evasion,[20] and regulate securities exchanges to protect investors. Some commentators argue that the public ledger has the potential to "eliminate intermediaries without eliminating the underlying conduct."[21] If that is the case, then regulators would lose the ability to use intermediaries as regulatory agents.[22] In theory, this would necessitate the regulation of dispersed crowds—meaning direct regulation of individuals who participate in financial markets. Such regulation is immensely costly—a problem exacerbated by the fact that the users, as explained above, are relatively anonymous. The combination of anonymity and the decentralization of financial dealings presents governments with formidable regulatory challenges.

---

[18] See Craig K. Elwell, M. Maureen Murphy, and Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues* *3 (Congressional Research Service July 15, 2014), online at http://fas.org/sgp/crs/misc/R43339.pdf (visited Nov 16, 2014).

[19] See generally Malte Möser, *Anonymity of Bitcoin Transactions: An Analysis of Mixing Services* (University of Münster Working Paper, 2013), online at https://www.wi.uni-muenster.de/sites/default/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf (visited Nov 16, 2014). See also Dorit Ron and Adi Shamir, *Quantitative Analysis of the Full Bitcoin Transaction Graph*, in Ahmad-Reza Sadeghi, ed, *Financial Cryptography and Data Security* 6 (Springer 2013).

[20] See Europol, *iOCTA* at *42 (cited in note 15); IRS, *Withholding Agent*, (Nov 14, 2014), online at http://www.irs.gov/Individuals/International-Taxpayers/Withholding-Agent (visited Nov 18, 2014).

[21] Brito, Shadab, and Castillo, 16 Colum Sci & Tech L Rev at *71 (cited in note 2).

[22] See Yee, 3 Internet Pol Rev at 4–5 (cited in note 2).

Some skepticism about the elimination of intermediaries from cryptocurrency markets is warranted, however.[23] Intermediaries are market-created, not government-created, constructs. Intermediaries do not just serve as agents for buyers and sellers but in fact add value to financial markets.[24] The cryptocurrency market demands the creation of new financial intermediaries to serve it. Such intermediaries include exchanges of cryptocurrencies to fiat currencies, cryptocurrency-wallet service providers, and clearinghouses for cryptocurrency transactions.[25] These new intermediaries can be subjected to traditional models of intermediary regulation, and indeed they have been. For example, the Treasury's Financial Crimes Enforcement Network subjects certain cryptocurrency service providers to regulations as money transmitters,[26] the IRS requires certain cryptocurrency clearing organizations to provide information to the IRS and their service recipients,[27] and the New York State Department of Financial Services recently proposed rules that would require registration and licensing for certain cryptocurrency financial services providers.[28] This Essay proceeds under the assumption that many new intermediaries would be subjected to traditional regulatory models. The main contribution of this Essay is in the context of transactions in which traditional intermediaries may become obsolete.

---

[23] See David S. Evans, *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms* *14–16 (University of Chicago Coase-Sandor Institute for Law and Economics Research Paper No 685, Apr 15, 2014), online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424516 (visited Nov 19, 2014).

[24] See generally Franklin Allen and Anthony M. Santomero, *What Do Financial Intermediaries Do?*, 25 J Bank & Fin 271 (2001). For the role of intermediaries in the context of online markets, see generally George M. Giaglis, Stefan Klein, and Robert M. O'Keefe, *The Role of Intermediaries in Electronic Marketplaces: Developing a Contingency Model*, 12 Info Systems J 231 (2002).

[25] See Tyler Moore and Nicolas Christin, *Beware of the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, in Sadeghi, ed, *Financial Cryptography* 25, 26 (cited in note 19).

[26] US Department of Treasury, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* *3 (FinCEN Mar 18, 2013), online at http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (visited Nov 19, 2014).

[27] IRS, *Notice 2014-21* *5–6 (Mar 25, 2014), online at http://www.irs.gov/pub/irs-drop/n-14-21.pdf (visited Nov 19, 2014).

[28] See New York Department of Financial Services, *Proposed New York Codes, Rules and Regulations: Virtual Currencies* *6 (July 17, 2014), online at http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf (visited Nov 16, 2014).

II. CRYPTOCURRENCIES AND THE UTILITY OF CRIMINAL BEHAVIOR

A. Basic Assumptions

This Essay argues that regulation should not prevent cryptocurrencies from achieving their positive potential. On the other hand, regulation *should* prevent cryptocurrencies from becoming a vehicle for criminal activity. Therefore, regulation of cryptocurrencies should not treat any cryptocurrency as a homogeneous instrument. Rather, the idea is to deconstruct cryptocurrencies into their unique traits, dealing with their vices and virtues separately. For example, decentralization is a positive trait that should not be disrupted. Anonymity should be targeted only to the extent that it *increases* the likelihood that individuals use cryptocurrencies to engage in criminal behavior.

Accordingly, this Essay proceeds under the following assumptions and qualifications: First, the current level of criminal activity in the market is taken as a benchmark. Regulating cryptocurrencies is not intended to reduce the current level of criminal activity but rather to ensure that cryptocurrencies do not *increase* criminal activity. Second, it is assumed that financial anonymity has an independent normative appeal even though it may facilitate criminal behavior.[29] The current status of financial anonymity is taken as a benchmark—any regulatory framework should not *decrease* the current level of financial anonymity. However, regulation is also not aimed at increasing the level of anonymity. Finally, the regulatory framework assumes that, if no new regulatory costs are imposed on the legitimate use of cryptocurrencies, the market will allow the new technology to develop to the extent that it offers benefits (other than anonymity) that fiat currencies do not.

B. Addressing the Utility of Cryptocurrencies in Criminal Behavior

Under the classic utility model of criminal behavior suggested by Professor Gary S. Becker, a rational, profit-seeking

---

[29] See Jim Harper, *Removing Impediments to Bitcoin's Success: A Risk Management Study* *5 (Bitcoin Foundation Research Brief No 1, 2014), online at https://bitcoinfoundation.org/static/2014/04/Bitcoin-Risk-Management-Study-Spring-2014.pdf (visited Nov 19, 2014).

individual will engage in criminal behavior if the utility of doing so is greater than zero (that is, greater than not engaging in criminal behavior).[30] In calculating the expected utility, an individual considers the expected gain from illicit behavior, the probability of being sanctioned, and the cost of any sanction that may be imposed.[31]

As noted above, the current level of criminal activity in the market is taken as a benchmark. This means that all individuals have already calculated their expected utility from criminal behavior and are either engaged or not engaged in criminal activity. The regulatory framework advanced in this Essay strives to *maintain* the current level of criminal behavior.

Assume now that cryptocurrencies are introduced. An individual who had previously calculated negative utility from engaging in criminal behavior using fiat currencies—and therefore was not engaged in criminal activity—is now presented with the option to use cryptocurrencies. Using cryptocurrencies to facilitate the previously contemplated illicit activity significantly reduces the probability of being sanctioned due to the anonymity associated with cryptocurrencies. Thus, if an individual expects to extract the same value from illicit behavior—meaning that the only difference is the denomination of the illicit gain—the utility function produces a greater expected outcome.[32]

Consequently, individuals who had previously calculated negative utility from engaging in criminal behavior might now calculate positive utility solely because the illicit activity is executed through the use of cryptocurrencies. Thus, in the absence of a regulatory response, a simple utility model predicts that the introduction of cryptocurrencies would increase the level of criminal activity, because more individuals would engage in it.

---

[30] See Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J Pol Econ 169, 176 (1968).

[31] Becker's basic utility function is expressed as follows:

$$E[U] = pU(Y - f) + (1 - p)U(Y)$$

Where E[U] is the expected utility from engaging in criminal behavior, p is the probability of facing criminal sanction, Y is the value expected to be generated from the criminal activity, and f is the cost of the criminal sanction. See id at 177 n 16.

[32] This assumes, of course, that the utility functions of fiat currencies and cryptocurrencies are identical, so that the utility of $\$X$ is equal to the utility of $\$X$ worth of cryptocurrencies. In reality, however, this assumption is probably overstated so long as cryptocurrencies are not widely adopted.

Governments' most obvious response would be to impose a stricter sanction in cases of illicit activity denominated in cryptocurrencies. Thus, if a criminal is sanctioned, he or she would face a tougher sanction if the gains were denominated in cryptocurrencies than if the same gains were denominated in fiat currencies. This could theoretically equate the utility of using cryptocurrencies with the utility of using fiat currencies in criminal activity. In such a case, the decision whether to engage in criminal behavior should not change on account of using cryptocurrencies versus fiat currencies, and the level of criminal activity would be maintained.

There are several problems, however, with imposing increased sanctions on such cryptocurrency-denominated gains. First, this approach means that two similarly situated criminals may face different sanctions if one used fiat currencies and the other used cryptocurrencies. There is a normative difficulty with imposing different criminal sanctions on functionally identical offenses simply because the gains are denominated in different units of account. Second, a vast body of literature questions the relationship between increased sanctions and the expected deterrence effect on criminal behavior. Many studies suggest that increasing the *probability* of sanction has a larger deterrent effect than increasing the *severity* of a sanction.[33]

However, increased sanction is not the only course of action that governments can take. The discussion thus far has assumed that the utility function of fiat currencies is identical to that of cryptocurrencies. Governments are in a position to alter this reality. For example, governments could design a quantity regulation that limits the ability of certain institutions to deal in cryptocurrencies.[34] When major market participants do not transact in cryptocurrencies, criminals are limited in their ability to use their illicit gains. In the alternative, governments could create price regulations that impose certain costs on dealings in cryptocurrencies in the open economy. For example, it is possible to impose a sales tax on certain cryptocurrency transactions when at least one of the parties to the transaction

---

[33] See, for example, Becker, 76 J Pol Econ at 176 (cited in note 30).

[34] China, for example, has banned certain financial institutions from handling cryptocurrency transactions. See *China Bans Financial Companies from Bitcoin Transactions*, (Bloomberg News Dec 5, 2013), online at http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html (visited Nov 19, 2014).

is known to the government and can therefore be the target of an enforcement action. This would force criminals to internalize excess costs when disposing of their illicit gains in the open economy.

Such regulatory impediments on the use of cryptocurrencies would make the expected utility of $\$X$ worth of a cryptocurrency *lower* than the utility of $\$X$. Thus, some individuals who found it cost-justified to engage in criminal behavior via cryptocurrencies before the introduction of regulation would not do so after the introduction of regulation, notwithstanding the fact that the probability of sanction would be lower.

The obvious shortcoming of such regulatory impediments is that they would also apply when cryptocurrencies are used for legitimate purposes. If cryptocurrency transactions are subjected to regulatory costs and fiat-currency transactions are not, a rational, *law-abiding* individual would never use cryptocurrencies. This might stifle innovation arising from cryptocurrencies. It would also create an adverse-selection problem—under such circumstances, wrongdoers are expected to be the primary adopters of cryptocurrencies. This is not a desirable result.

In order to solve this problem, this Essay suggests that any regulatory cost associated with the use of cryptocurrencies be conditioned on anonymity. In essence, an individual transacting in cryptocurrencies in the open economy would elect between bearing the cost of regulation and waiving the trait that makes cryptocurrencies suited for illicit behavior—anonymity. For example, merchants would be permitted to accept cryptocurrencies, provided that the other party to a transaction identified herself as the owner of the cryptocurrency address used in that transaction. This could be achieved by requiring purchasers to sign transaction receipts or by using a private identification number, as is done today in debit and credit card transactions. A stronger version of the same idea would be to prohibit the use of any cryptocurrency that had ever been transferred without adequate disclosure[35] or that had ever been associated with an unknown public address.

In such a case, there is no increased cost for transacting in cryptocurrencies compared with transacting in fiat currencies. However, the probability of detection of any criminal activity associated with the cryptocurrency address used to transact is no

[35] I am indebted to Professor Michael Abramowicz for this innovative idea.

longer diminished because the owner of the address is known. Thus, to the extent that it is preferable to use cryptocurrencies for reasons that are not associated with anonymity, cryptocurrency use should flourish.

Finally, under such an approach, the status quo level of financial anonymity is maintained. The regulatory framework should require that cryptocurrency users who elect to avoid the regulatory cost provide information to the same extent as required when using other financial accounts. For example, instead of providing information to a credit card company, the user would be allowed to provide information directly to the merchant, or to a third-party clearing organization that clears cryptocurrency transactions for the merchant.

Such a regulatory framework has an important derivative benefit. It not only addresses individuals' incentive to use cryptocurrencies for illicit purposes, but it potentially makes the cryptocurrency protocol as a whole less appealing for illicit users. Specifically, a unique feature of many cryptocurrencies' protocols is that the anonymity of all users—legitimate and illicit—is interconnected. As explained above, if the owners of some addresses are known, the public ledger can be used to identify owners of *other* addresses. The more addresses that are identified, the easier it is to identify other addresses (if there is a need to do so). Thus, a regulatory framework that incentivizes legitimate users to give up their anonymity will produce a cascade effect: the more users that identify themselves, the less anonymous the entire system becomes.

Theoretically, in order for the cascade effect to be meaningful, some critical mass of legitimate users would have to give up their anonymity in order for the system to become nonanonymous enough to deter illicit activity. The difficulty here is that the number of wallets that users can create is endless, and therefore additional legitimate users would have to continuously give up their anonymity. However, this could be mitigated if the fact that users voluntarily give up their anonymity is made salient. If illicit users were confronted with a reality in which other users give up their anonymity, then those illicit users would never be able to tell whether a required critical mass of identified users had been met. If this fact were salient enough, illicit users should be sufficiently discouraged from using cryptocurrencies' protocols. Under such a framework, legitimate users

passively participate in regulatory efforts to prevent illicit behavior.

III. AN EXAMPLE: AN ELECTIVE ANONYMITY TAX IN CRYPTOCURRENCY TRANSACTIONS

Our tax-collection system is based on individual self-reporting. The enforcement of such reporting requirements is largely dependent on the regulation of intermediaries. For example, various provisions in tax laws and regulations require financial institutions to identify their account holders. Based on the identity of the account holders, these institutions may be required to withhold taxes on payments made to such account holders and provide information about such account holders to the IRS.[36] The intermediaries are also required to provide the account holder with information necessary to complete the account holder's own tax return, generally on an IRS Form 1099. However, many taxable transactions that are traditionally facilitated through financial institutions can theoretically rely on cryptocurrency protocols in order to avoid the use of a costly financial intermediary and, as such, defeat intermediary-based tax enforcement.[37]

For example, a consumer can use cryptocurrency the same way that he or she uses cash. But, unlike cash, the disposition of a bitcoin is a taxable transaction to the consumer.[38] Under recent IRS guidance, cryptocurrency is "property" in the hands of a taxpayer, which means that its disposition is a taxable event to the extent that the cryptocurrency's value has changed since its acquisition by the taxpayer.[39] Because no intermediaries are involved, the collection of such tax is possible only to the extent that the taxpayer voluntarily reports such transactions.

However, a mechanism could be instituted to incentivize consumers to identify themselves to a merchant or to an intermediary that provides cryptocurrency clearing services. Under such a model, the merchant would function as a surrogate for the collection of what is presumed to be the purchaser's tax liability in the transaction (similar to the collection of sales taxes). Such a model can be referred to as "surrogate

---

36 See Marian, 112 Mich L Rev First Impressions at 39 (cited in note 17).

37 See id.

38 See IRS, *Notice 2014-21* *2 (cited in note 27).

39 Id.

presumptive collection."[40] Merchants that accept cryptocurrencies as a form of payment would be required to collect a special cryptocurrency-transaction tax based on a percentage of the gross value of any cryptocurrency payment and remit such tax to the IRS. This gross tax would be waived, however, if the consumer were identified by the merchant or by an approved third-party provider that cleared cryptocurrency payments for the merchant. The consumer would effectively be in a position to elect between avoiding the tax by disclosing his or her identity and paying the gross tax to maintain his or her anonymity.

If the consumer refused to be identified, the gross tax would serve as a proxy for what is functionally unreported income by the consumer, and the consumer would be presumed to have satisfied any tax liability associated with the transaction. In the alternative, no tax would be imposed if the consumer identified him or herself, under the assumption that, once the consumer's identity is exposed, he or she would have an incentive to properly report the income from the transaction.

The gross tax should be set at a rate that is more likely to result in overcollection of taxes, so as to incentivize consumers to identify themselves, or otherwise force them to internalize the cost of their tax evasion. If the tax rate is set correctly, consumers who would not have engaged in tax evasion using traditional payment methods should not be incentivized to do so using cryptocurrencies. To the extent that cryptocurrencies offer unique benefits other than anonymity (such as avoiding the need to deal with exchange rates), consumers should opt for using cryptocurrencies.

IV. CRITIQUE

Notwithstanding the primordial nature of the discussion, several critiques of the proposed framework should be noted. The first possible critique is a normative one: Cryptocurrencies offer an opportunity for increased financial anonymity, which can be viewed as a normatively desirable goal. However, anonymity is also expected to increase the level of criminal activity.[41] The framework presented in this Essay thus

---

[40] The term "presumptive collection" was coined by Professor Kathleen DeLaney Thomas. See generally Kathleen DeLaney Thomas, *Presumptive Collection: A Prospect Theory Approach to Increasing Small Business Tax Compliance*, 67 Tax L Rev 111 (2013).

[41] See text accompanying notes 15–19.

normatively rejects increased anonymity in favor of maintaining extant levels of criminal activity (but allows other innovative features of cryptocurrencies, such as decentralization). This choice can be criticized on ideological grounds.

The framework can also be criticized on technical grounds. If individuals can create as many cryptocurrency addresses as they desire, then they may create different addresses for criminal and legitimate activities. Individuals who have opted to commit crimes will use "known" wallets for their legal activity and "hidden" wallets for their illegal activity. The response is that the utility of any cryptocurrencies in hidden addresses will be diminished, since hidden-wallet cryptocurrencies could be used only to facilitate other criminal behavior but would be barred from use in the open market. In order to avoid this limitation, hidden cryptocurrencies would have to be moved from hidden to known addresses, at which point the owner of the hidden address could be traced using the public ledger.

Another possible critique of the above framework is that it assumes a certain market structure in which multiple known parties adopt bitcoin. An inherent limitation of the proposed framework is that it is applicable *only* when cryptocurrencies are used to transact with such known parties. Theoretically, then, if very few known merchants adopt cryptocurrencies, the functionality of the regulatory framework would be limited. This observation should not prove particularly damaging, however, for three reasons. First, merchants are increasingly adopting cryptocurrencies. For example, over the past two years, Dell, Dish Network, Expedia, Overstock, and other major retailers have all started to accept bitcoin as a form of payment.[42] These retailers can be a focal point of regulatory effort. Bitcoin has also been largely integrated into existing payment mechanisms such as PayPal.[43] Such intermediaries can also be used as regulatory agents. Second, to the extent that cryptocurrencies do remain isolated from open markets, cryptocurrencies are unlikely to present a significant regulatory problem, as their economic scale would remain rather small. If the cryptocurrency economy is to

---

[42] See Sydney Ember, *Dell Begins Accepting Bitcoin*, DealBook (NY Times July 18, 2014), online at http://dealbook.nytimes.com/2014/07/18/dell-begins-accepting-bitcoin (visited Nov 16, 2014).

[43] See Ryan Mac, *PayPal Takes Baby Step toward Bitcoin, Partners with Cryptocurrency Processors*, (Forbes Sept 23, 2014), online at http://www.forbes.com/sites/ryanmac/2014/09/23/paypal-takes-small-step-toward-bitcoin-partners-with-cryptocurrency-processors (visited Nov 17, 2014).

succeed, it must be used to interact with physical commodities and real services—namely, with real people who can be identified by regulators. In other words, if cryptocurrencies are not significantly adopted in the open market, then their utility is diminished compared with fiat currencies and the regulatory challenge remains minimal. Third, as noted above, to the extent that cryptocurrencies do become significant economic instruments, intermediaries will emerge. "In reality, most people will rely on intermediaries . . . when they use [cryptocurrencies]."[44] Most users (both merchants and consumers) are not tech experts and will naturally turn to intermediaries to dispose of their cryptocurrencies. Such intermediaries can be used, for example, to enforce the proposed tax.

Finally, the proposed framework could theoretically collapse if cryptocurrencies' protocols become completely anonymous. Several projects are aimed at taking the "public" out of the "public ledger," making all decentralized transfers completely anonymous by masking the addresses used in the transfers.[45] If such projects are successful, it would be impossible to build a transaction graph in order to trace transfers, and the entire regulatory approach would collapse. This Essay dismisses the idea that a *completely* anonymous financial system (that is, a system in which parties to a transaction are not known to each other) can succeed at all. It is devoid of an essential component of successful financial markets: trust. Completely anonymous cryptocurrencies may successfully function as a unit of account among criminals, but not in the context of transactions that require trust among parties. It is doubtful that such cryptocurrencies can induce noncriminals to become criminals, as the utility of these currencies would be significantly diminished.

CONCLUSION

This Essay decoupled cryptocurrencies into their two unique components: anonymity and decentralization. It then proposed a regulatory framework that targets the former and protects the latter, by adopting regulatory instruments that impose costs only on anonymity. Such a framework impedes the use of crypto-

---

[44] Yee, 3 Internet Pol Rev at 5 (cited in note 2).

[45] One such project is Darkcoin. See Darkcoin, *What is Darkcoin?*, (2014), online at https://www.darkcoin.io/about/what-is-darkcoin (visited Nov 11, 2014).

currencies in illicit activity but allows for legitimate uses of cryptocurrencies.

A full inquiry into the regulation of cryptocurrencies is beyond the scope of this Essay. Many important issues—such as regulatory-design choices, behavioral incentives, and the analysis of costs and benefits—remain for future research. However, the proposed framework offers a rallying point for future discussion on the design of regulatory instruments seeking to control the use of cryptocurrencies. The suggested framework also offers two new insights: First, it is conceivable to design regulatory instruments that target only the negative traits of cryptocurrencies while allowing positive traits to flourish. Second, it is possible to leverage the unique nature of the public ledger to enlist legitimate users as passive participants in regulatory efforts.