University of Florida Journal of Law & Public Policy

Volume 28 | Issue 1 Article 6

2017

# Crypto-Currencies: The 21st Century's Money Laundering and Tax Havens

Edgar G. Sanchez

# NOTES

## CRYPTO-CURRENCIES: THE 21ST CENTURY'S MONEY LAUNDERING AND TAX HAVENS

*Edgar G. Sánchez**



---

* J.D. 2017, University of Florida Levin College of Law. I would like to thank my mother, Carmen Sánchez, and father, Edgar Sánchez, for all their love, support, and constant encouragement throughout the years. I would like to thank my sister, Paola Sánchez, for having taught me the patience needed to deal with the many challenges in life. In addition, I would also like to thank my friends for their constant enthusiasm and encouragement. Last, I would like to extend my sincerest gratitude to Professor Taryn Marks for her guidance and support throughout my legal education.

Mostly gone are the days where money laundering involved "washing" money through casinos, offshore banks, and shell corporations.[1] With the creation of the Internet came innovative new tactics through which individuals can remain anonymous and control the movement of their money, all while avoiding taxes.[2] The newest of these schemes is to convert money into crypto-currencies;[3] the most well-known crypto-currency is Bitcoin.[4]

1. Diane Francis, *A Beginner's Guide to Laundering Money*, BUSINESS INSIDER (Oct. 9, 2014, 11:24AM), http://www.businessinsider.com/beginners-guide-to-money-laundering-2014-10.

2. *Id.*

3. "A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank . . . ."*Cryptocurrency*, Oxford Dictionary British & World English, https://en.oxforddictionaries.com/definition/cryptocurrency (last visited Nov. 1, 2016). "A cryptocurrency is a digital or virtual currency that uses cryptography for security. A cryptocurrency is difficult to counterfeit because of this security feature." Furthermore, its defining feature is that "it is not issued by any central authority rendering it theoretically immune to government interference or manipulation." *Cryptocurrency*, INVESTOPEDIA, http://www.investopedia.com/terms/c/cryptocurrency.asp?ad=dirN&qo=InvestopediaSiteSearch&qsrc=0&o=40186.

4. David Z. Morris, *IRS Requests Bitcoin Buyer Records in Broad Tax Evasion Case*, FORTUNE (Nov. 20, 2016, 4:14 PM), http://fortune.com/2016/11/20/irs-bitcoin-tax-evasion-case/.

Since its inception in October 2008, the value of a bitcoin[5] has increased from a fraction of a penny to over seven hundred dollars per bitcoin.[6] Its demand and versatility have led to it being accepted to purchase items or services ranging from pizzas to hit men.[7] However, the newest growing concern with Bitcoin, and crypto-currencies in general, are their ability to wash money and conceal taxable income.[8]

Although at the individual level the consequences of money laundering and tax evasion may seem trivial and often times go undetected, the reality is that their overall consequences on society as a whole are ever increasing. To name a few, first, they deprive a nation from raising sufficient revenues.[9] The result of this is that it frustrates a nation's ability to implement social, economic, and other policies. Additionally, it undermines a nation's ability to promote social welfare.[10] Second, those who evade paying taxes place the burden on those who pay their taxes.[11] The consequences of this are a greater tax burden on law-abiding taxpayers, and a widening of economic inequality.[12] Third, it encourages corruption in banks and financial institutions.[13] Fourth, and finally, by disguising and diverting income to other nations, it deprives a nation from acquiring taxable funds and creates unfair fiscal competition between nations.[14]

Considering the consequences of money laundering and tax evasion, it is imperative to assess how the United States is targeting industries, especially in this case, crypto-currency exchanges that facilitate these practices. This Note will analyze the U.S. response to the use of crypto-

---

5. "According to the official Bitcoin Foundation, the word 'Bitcoin' is capitalized in the context of referring to the entity or concept, whereas 'bitcoin' is written in the lower case when referring to a quantity of the currency." *Bitcoin*, INVESTOPEDIA, http://www.investopedia.com/terms/b/bitcoin.asp.

6. *An Abriged History of Bitcoin*, N.Y. TIMES (Nov. 19, 2013), http://www.nytimes.com/interactive/technology/bitcoin-timeline.html#/#time284_8156.

7. Donna Leinwand Leger, *How FBI Brought Down Cyber-Underworld Site Silk Road*, USA TODAY (May 15, 2014, 2:54PM), http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/.

8. Laura Shin, *Bitcoin at Tax Time: What You Need to Know About Trading, Tipping, Mining and More*, FORBES (Dec. 16, 2015, 7:00AM), http://www.forbes.com/sites/laurashin/2015/12/16/bitcoin-at-tax-time-what-you-need-to-know-about-trading-tipping-mining-and-more/#307c4cd36692.

9. Rui Tavares, *Thematic Paper on Money Laundering: Relationship Between Money Laundering, Tax Evasion and Tax Havens*, SPECIAL COMM. ON ORGANISED CRIME, CORRUPTION AND MONEY LAUNDERING 2012-2013, at 1, 3 (Jan. 2013), http://www.europarl.europa.eu/meetdocs/2009_2014/ documents/crim/dv/tavares_ml_/tavares_ml_en.pdf.

10. *Id.* at 2-3.

11. *Id.* at 3.

12. *Id.*

13. *Id.*

14. *Id.*

currencies to launder money and evade taxes. This Note will then analyze the regulations that government agencies have promulgated in response to crypto-currencies expanding use. This Note next will argue that the Department of the Treasury, specifically the Financial Crimes Enforcement Network, should change its classification of crypto-currencies in order to require them to comply with the Bank Secrecy Act. In the alternative, this Note will argue that crypto-currency exchanges need to keep personal records of their users in order to facilitate the IRS financial investigations of money laundering and tax evasion.

This Note is broken-down as follows. Part I will provide a general overview of money laundering. Part II will provide a general overview of tax evasion. Part III will provide a general overview of the economic consequences of money laundering and tax evasion. Part IV will provide a general overview of crypto-currencies, more specifically, of Bitcoin. Part V will provide a general overview of the U.S. treatment of crypto-currencies. Finally, Part VI will propose solutions to regulate crypto-currencies in order to diminish their abuse to launder money and evade taxes.

## I. WHAT IS MONEY LAUNDERING?

In general, "'money laundering' refers to the activities and financial transactions that are undertaken specifically to hide the true source of the money. In most cases, the money involved is earned from an illegal enterprise and the goal is to give that money the appearance of coming from a legitimate source."[15]

The purpose of changing the appearance of illegally acquired money is to allow the individual to spend it or invest it without having to worry about interference from Authorities or the Internal Revenue Service.[16] Furthermore, by disguising the money, an individual is able to bypass income tax consequences by circumventing Internal Revenue Code, Section 61(a), which requires an individual to include in their taxable income "all income from whatever source derived," this includes any income received from illegal activities.[17]

In practice, two different types of money laundering transactions exist

15. INTERNAL REVENUE SERVICE, *Overview – Money Laundering* (Apr. 29, 2016), https://www.irs.gov/uac/overview-money-laundering.

16. *Id.*

17. 26 U.S.C. § 61(a) (2016). *See also* INTERNAL REVENUE SERVICE, *Federal Statutes – Money Laundering* (Dec. 9, 2016), https://www.irs.gov/uac/federal-statutes-money-laundering.

that intertwine with tax evasion:[18] *domestic* money laundering[19] and *international* money laundering.[20]

### A. *Domestic Money Laundering*

Domestic money laundering is the simplest form of money laundering. It involves a financial transaction in which an individual successfully completes or attempts to complete the transaction with knowledge that the property involved was derived as proceeds from unlawful activity.[21] Examples of unlawful activities are defined in the United States Code Section 1956(c)(7).[22]

#### 1. Financial Transaction

A financial transaction is defined as a transaction which affects interstate or foreign commerce and involves either the movement of funds by wire or other similar means; the use of one or several monetary instruments; or the transfer of title to real property, including transfers of title of a vehicle, vessel or aircraft.[23] A financial transaction also includes a transaction, which involves the use of a financial institution that is engaged in or can affect interstate or foreign commerce.[24]

#### 2. Intent or Knowledge

The pertinent key elements of domestic money laundering that intertwine with tax evasion are that the individual who carried out the transaction had either the *intent* to violate Sections 7201 or 7206 of the Internal Revenue Code[25] or had *knowledge* that the transaction was designed "to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity."[26]

---

18. OFFICE OF THE U.S. ATTORNEYS, CRIMINAL RESOURCE MANUAL § *2101. Money Laundering Overview*, (1997), https://www.justice.gov/usam/ criminal-resource-manual-2101-money-laundering-overview.
19. 18 U.S.C. § 1956(a)(1) (2016).
20. 18 U.S.C. § 1956(a)(3) (2016).
21. 18 U.S.C. § 1956(a)(1) (2016).
22. 18 U.S.C. § 1956(c)(7) (2016).
23. 18 U.S.C. § 1956(c)(4) (2016).
24. *Id.*
25. 18 U.S.C. § 1956(a)(1)(A)(ii) (2016) (citing I.R.C. §§ 7201, 7206 (2016)).
26. 18 U.S.C. § 1956(a)(1)(B)(i) (2016).

### 3. Punishment for Domestic Money Laundering

The consequences of domestic money laundering vary. One penalty is the greater of either a fine of 500,000 dollars or twice the value of the property that was used by the individual in the transaction.[27] Alternatively, an individual can be imprisoned for up to twenty years.[28] In the worst-case scenario, an individual may receive both punishments.[29] Furthermore, in situations where an individual has been tried for various transactions, each transaction is charged separately.[30] Thus, each time an individual moves a piece of property that was derived as proceeds from unlawful activity, even if it is the same piece of property, that individual is committing a new offense that can be charged independently.[31]

## B. *International Money Laundering*

International money laundering is similar to domestic money laundering, but contains some key differences. The first difference is that it involves only monetary instruments or funds.[32] Second, international money laundering involves a financial transaction in which an individual successfully completes or attempts to complete a transaction from a location "in the United States to or through a place outside the United States."[33] In the alternative, it involves a transaction "to a place in the United States from or through a place outside the United States."[34]

### 1. Monetary Instrument or Funds

A monetary instrument is coins or currency of any country.[35] It includes "travelers' checks, personal checks, bank checks, and money orders."[36] In addition, investment securities and other negotiable instruments that pass title upon delivery are also considered monetary instruments.[37]

---

27. 18 U.S.C. § 1956(a)(1)(B) (2016).
28. *Id.*
29. *Id.*
30. *See, e.g.*, United States v. Prescott, 42 F.3d 1165 (8th Cir. 1994); United States v. Conley, 826 F. Supp. 1536 (W.D. Pa. 1993).
31. *Supra* text accompanying note 18 ("For example, [] an individual earns $100,000 from [an] offense. If he then withdraws $50,000, he commits a second offense. If he then purchases a car with the withdrawn $50,000, he commits a third offense.").
32. 18 U.S.C. § 1956(a)(2) (2016).
33. *Id.*
34. *Id.*
35. 18 U.S.C. § 1956(c)(5) (2016).
36. *Id.*
37. *Id.*

### 2. Knowledge

The pertinent key elements of international money laundering that intertwine with tax evasion are that the individual *knowingly* transported, transmitted, or transferred the monetary instrument or funds that were derived from unlawful activities in order "to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds."[38]

### 3. Punishment for International Money Laundering

The consequences of international money laundering parallel those of domestic money laundering. An individual convicted of international money laundering can either be fined, sentenced to imprisonment, or both.[39]

The Internal Revenue Service has taken the position that because money laundering and tax evasion are so interrelated they are always committed simultaneously.[40] Specifically, the Internal Revenue Service has concluded that any criminal investigation that focuses on money laundering is the result of underlying conduct that has violated the income tax laws[41] or the Bank Secrecy Act.[42] The reason for this is because money laundering, the means by which individuals avoid paying taxes on income by concealing its source and profit, is tax evasion in progress.[43] Considering the Internal Revenue Service's assertion that both money laundering and tax evasion are interrelated, it is now imperative to analyze the concept of tax evasion.

## II. WHAT IS TAX EVASION?

Prior to assessing tax evasion, it is necessary to keep in mind two things about the U.S. tax system. First, the U.S. tax system creates a distinction between tax evasion, which is a criminal act, and tax avoidance, which is not a criminal offense.[44] Second, the U.S. tax system is largely based on voluntary compliance because it places the responsibility on the individual to assess and report their tax liability.[45]

---

38. 18 U.S.C. § 1956(a)(2)(B)(i) (2016).
39. 18 U.S.C. § 1956(a)(2)(B) (2016).
40. *Supra* text accompanying note 15.
41. *Id.*
42. *Id.*
43. *Id.*
44. INTERNAL REVENUE SERVICE, PART 9. CRIMINAL INVESTIGATION, https://www.irs.gov/irm/part9/irm_09-001-003.html.
45. INTERNAL REVENUE SERVICE, FINANCIAL INVESTIGATION – CRIMINAL INVESTIGATION

Due to this voluntary compliance aspect, the Internal Revenue Service will only exercise its enforcement authority when evidence exists that an individual is evading taxes.[46] Thus, if an individual can successfully disguise their income, the Internal Revenue Service will have no evidence to enforce the tax evasion statutes.[47]

The Internal Revenue Code section 7201 is the governing tax evasion statute.[48] In general, section 7201 lists the consequences of attempting to evade or successfully defeating a tax regulation.[49] However, section 7201 does not provide a clear explanation as to what constitutes tax evasion.[50] Nonetheless, the Supreme Court has concluded that section 7201 describes two kinds of tax evasion.[51] First, an individual may commit tax evasion by "willfully attempting to evade or defeat the *assessment* of a tax."[52] In the alternative, an individual may commit tax evasion by "willfully attempting to evade or defeat the *payment* of a tax."[53]

### A. *Willful Attempt to Evade or Defeat the Assessment of a Tax*

An evasion of an *assessment* is the most common type of tax evasion.[54] Under this offense an individual typically files a return that omits income.[55] Alternatively, an individual may submit a fraudulent return claiming deductions that the individual is not entitled to.[56] The result is that the fraudulent return understates the individual's true taxable amount, thus creating a deficiency.[57]

---

(CI), https://www.irs.gov/uac/financial-investigations-criminal-investigation-ci.

46. *Id.*

47. *Id.*

48. 26 U.S.C.A § 7201. (2016)

49. *Id.*

> Any person who willfully attempts in any manner to evade or defeat any tax imposed by this title or the payment thereof shall, in addition to other penalties provided by law, be guilty of a felony and, upon conviction thereof, shall be fined not more than $100,000 ($500,000 in the case of a corporation), or imprisoned not more than 5 years, or both, together with costs of prosecution.

*Id.*

50. *Id.*

51. Sansone v. United States, 380 U.S. 343, 354 (1965).

52. *Id.* (emphasis added).

53. *Id.* (emphasis added).

54. EDWARD F. CRONIN, OFFICE OF CHIEF COUNSEL CRIMINAL TAX DIVISION, *Tax Crimes Handbook*, (2009), https://www.irs.gov/pub/irs-utl/tax_ crimes_handbook.pdf.

55. *Id.* at 2.

56. *Id.*

57. *Id.*; *Deficiency*, BLACK'S LAW DICTIONARY (4th ed. 2011) ("A shortfall in paying taxes; the amount by which the tax properly due exceeds the sum of the amount of tax shown on a taxpayer's return.").

### B. *Willful Attempt to Evade or Defeat the Payment of a Tax*

On the other hand, an evasion of *payment* only occurs after the amount of tax due by an individual has been established.[58] In this case, an individual either must have reported the amount of tax owed or the Internal Revenue Service must have performed an assessment of the amount of tax owed by an individual.[59] Subsequent to either of these two events, the individual evades payment of the established taxes by concealing money or assets from which the tax could be satisfied.[60]

### C. *Consequences of Tax Evasion*

The consequences for tax evasion are either a fine of $100,000 for individuals or $500,000 in the case of corporations, plus costs of prosecution.[61] An additional consequence is the imprisonment of an individual for up to five years, plus costs of prosecution.[62] Lastly, a court has the discretion to combine the punishments.[63]

### D. *Tax Avoidance*

Unlike tax evasion, tax *avoidance* involves a legitimate attempt to reduce, avoid, minimize, or alleviate taxes currently owed; tax avoidance may also include attempts related to what would be owed as a result of the unfolding of taxable events.[64] The defining feature between evasion and avoidance is that avoidance of a tax does not require an individual to conceal or misrepresent their income or ability to pay an outstanding debt.[65] Rather, in order to avoid a tax, an individual shapes taxable events in a manner that results in a reduction or complete elimination of tax liability in accordance with statutory precedent.[66] Most importantly in tax avoidance, the individual makes full disclosure of the events as they occur.[67]

In essence, the main difference between avoidance and evasion is that evasion requires "deceit, subterfuge, camouflage, concealment, [and] some attempt to color or obscure events to make things seem other than

---

58. CRONIN, *supra* note 54, at 2.
59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.*
63. *Id.*
64. *I.R.M. § 9.1.3.3.2.1,* Avoidance Distinguished from Evasion, https://www.irs.gov/irm/part9/irm_09-001-003.html.
65. *Id.*
66. *Id.*
67. *Id.*

they are," while avoidance requires full disclosure and strategic planning that follows statutory guidelines.[68] Although the outcomes of both scenarios lead to an individual paying less in taxes than what is originally intended by the Internal Revenue Service, the key difference is that tax evasion entails following statutory precedent which actually intends for an individual to reduce their taxes lawfully.[69]

## III. ECONOMIC CONSEQUENCES OF MONEY LAUNDERING AND TAX EVASION

Due to its secrecy, the costs of money laundering and tax evasion in global and national economies are largely unknown. However, the United Nations and the United States perform periodic retroactive studies to assess the impact of these activities.

### A. *Money Laundering Estimates*

In 2011, the U.N. Office on Drugs and Crime performed a retroactive study that concentrated on estimating the illicit financial flows of money that were derived from drug trafficking and organized crime.[70] The study estimated that criminal income in the United States in 2010, *not including* tax evasion, was as much as $350 billion, most of which was laundered within the United States.[71] Furthermore, the study concluded that in 2009, approximately $2.1 trillion were global crime proceeds.[72] It further estimated that $1.6 trillion were successfully laundered.[73] This amounted to approximately 2.7% of the global gross domestic product (GDP) being

---

68. *Id.*

> For example, the creation of a bona fide partnership to reduce the tax liability of a business by dividing the income among several individual partners is tax avoidance. However, the facts of a particular investigation may show that an alleged partnership was not, in fact, established and that one or more of the alleged partners secretly returned his/her share of the profits to the real owner of the business, who, in turn, did not report this income. This would be an instance of attempted evasion.

*Id.*

69. *Id.*

70. U.N. OFFICE ON DRUGS AND CRIME, ESTIMATING ILLICIT FINANCIAL FLOWS RESULTING FROM DRUG TRAFFICKING AND OTHER TRANSNATIONAL ORGANIZED CRIMES (Oct. 2011), http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

71. *Id.* at 20.

72. *Id.* at 99.

73. *Id.* at 127.

successfully laundered.

In a similar 2015 study, the U.S. Department of the Treasury released its *National Money Laundering Risk Assessment* study that estimated approximately $300 billion were derived from all forms of financial crime within the United States.[74] This amount consisted of approximately $64 billion in illicit drug sales and about $236 billion derived from all other forms of financial crime in the United States, the majority of which came from fraudulent activities.[75] However, this $300 billion estimate excluded any illegal proceeds that resulted from tax evasion.[76] Given the uncertainty of the estimates, the Treasury Department did not provide a formal estimate of how much of the $300 billion that had been derived from all forms of financial crime were successfully laundered in the United States.[77] Nonetheless, given the similarity with estimates provided by the U.N. Office on Drugs and Crime in 2010,[78] it can be assumed that a large portion of the $300 billion were successfully laundered within the United States.

### B. *Tax Evasion Estimates*

In 2012, the Internal Revenue Service released its *Tax Gap for Tax Year 2006* report, which estimated that the gross tax gap[79] was $450 billion.[80] The Internal Revenue Service estimated that of these $450 billion only $95 billion would be collected in subsequent years. Therefore the net tax gap for 2006,[81] which would never be collected, was $385 billion.[82] The Internal Revenue Service concluded that the 2006 estimates were an increase from its estimate of the 2001 gross tax gap, which was $345 billion, and its estimated 2001 net tax gap, which was $290 billion.[83]

In 2016, the Internal Revenue Service released its amended tax gap

---

74. ADAM J. SZUBIN, DEPARTMENT OF THE TREASURY, NATIONAL MONEY LAUNDERING RISK ASSESSMENT 2 (2015), https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

75. *Id.* at 11.

76. *Id.*

77. *Id.*

78. *See* discussion *supra* Part III.A.

79. *Tax Gap for Tax Year 2006*, INTERNAL REVENUE SERVICE (Jan. 6, 2012), https://www.irs.gov/pub/newsroom/overview_tax_gap_2006.pdf ("The *gross tax gap* is defined as the amount of true tax liability faced by taxpayers that is not paid on time.") (emphasis added).

80. *Id.*

81. "The *net tax gap* is defined as the amount of true tax liability that is not paid on time and is not collected subsequently, either voluntarily or as the result of enforcement activities. Thus, the *net tax gap* represents the amount of tax liability that is never paid." *Id.* (emphasis added).

82. *Id.*

83. *Id.*

report.[84] The report estimated how much money went uncollected in the years 2008 through 2010.[85] In its study, the Internal Revenue Service broke down the amounts not collected as a result of the three most common tax evasion scenarios: "nonfiling, underreporting, and underpayment."[86] It estimated that from 2008 to 2010, the annual gross tax gap was approximately $458 billion.[87] The Internal Revenue Service broke down the gross tax gap total and estimated that $32 billion went uncollected because of *nonfiling*, $387 billion went uncollected as result of *underreporting*, and $39 billion went uncollected because of *underpayment*.[88] Furthermore, the Internal Revenue Service estimated that of these $458 billion, only $52 billion would ever be collected, leaving an outstanding net tax gap of $406 billion per year.[89] The Internal Revenue Service concluded that this tax gap was an increase from previous tax years.[90] In sum, the study alludes to the fact that about $1.2 trillion in taxes will never be collected the years 2008 through 2010 as a consequence of individuals successfully committing tax evasion.[91]

## IV. WHAT ARE CRYPTO-CURRENCIES?

Often described as the currency of the future, crypto-currencies, in their most basic form, are "virtual currency" that may be used to pay for goods or services.[92] In recent years, these currencies have even allowed individuals to hold them as investments.[93] Although these currencies are digital representations of value, in some jurisdictions they are treated as real currency despite the fact that no jurisdiction officially considers them legal tender.[94]

Although virtual currency originally had no real world value, it eventually crossed the threshold into a representation of real currency.[95]

84. *Tax Gap Estimates for Tax Years 2008–2010*, INTERNAL REVENUE SERVICE (Apr. 2016), https://www.irs.gov/PUP/newsroom/tax%20gap%20estimates%20for%202008%20through%202010.pdf.

85. *See id.*

86. *Id.* at 2.

87. *Id.*

88. *Id.*

89. *Id.* at 1.

90. *Id.* at 2.

91. *See id.* My calculation took into account only the net tax gap, $402 billion, multiplied by 3, for each of the years 2008, 2009, and 2010. Thus, $406 billion (tax gap) multiplied by 3 (years) is $1,218 billion, or $1 trillion 218 billion in total for the years 2008 through 2010.

92. *Notice 2014-21*, INTERNAL REVENUE SERVICE (Apr. 14, 2014), https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

93. *Id.*

94. *Id.*

95. *Id.*

This new valuation concept came to be known as "convertible virtual currency," and is largely regulated by online exchanges commonly referred to as "crypto-currency exchanges."[96]

In essence, convertible virtual currency is virtual currency that has an equivalent value in real currency.[97] Due to its acceptance by the public as legal tender, despite it *not actually being* considered legal tender in any jurisdiction, convertible virtual currency can be purchased, traded, and converted into "real" currency such as U.S. dollars, Euros, and other real or virtual currencies.[98] Today, the most prevalent form of convertible virtual currencies is Bitcoin.

### A. *Bitcoin: A Brief History*

The idea of Bitcoin first rose to the surface in 2008.[99] An individual or group (it is unknown which specifically) named Satoshi Nakamoto published an article outlining the concept of a "peer-to-peer" electronic cash system.[100] This concept relied on software code to authenticate and protect transactions using an electronic medium that would represent value—"real" monetary value—in the hands of the holder.[101]

After its initial reception, the first Bitcoin transaction is said to have occurred in 2010.[102] A user by the name of Laszlo claimed to have purchased pizza using 10,000 bitcoins.[103] Quickly after this purchase, the Bitcoin craze hit the public, and in proceeding years the once-obscure virtual currency became one that was socially accepted by individuals.[104]

In light of the rather quick acceptance of the Bitcoin concept, its market value increased from fractions of a penny in its infancy to $266 in April 2013.[105] Today, an individual bitcoin is valued at around $754, and the total value of bitcoins in circulation is approximately $12.1 billion.[106] In light of its growing acceptance, its limited availability,[107] and the possible economic consequences of a new presidency, the price

---

96. *Id.*
97. *Id.*
98. *Id.*
99. *An Abridged History of Bitcoin*, N.Y. TIMES (Nov. 19, 2013), http://www.nytimes.com/interactive/technology/bitcoin-timeline.html#/#time284_8156.
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*
105. *Id.*
106. Arjun Kharpal, *Bitcoin Predicted to Rise 165% to $2,000 in 2017 Driven by Trump's 'Spending Binge' and Dollar Rally*, CNBC (Dec. 7, 2016, 5:48 AM), http://www.cnbc.com/2016/12/07/bitcoin-price-could-rise-to-2000-in-2017-driven-by-trump-policies-us-dollar-inflation-rocketing.html.
107. *Id.* (stating that a "*finite* supply of 21 million bitcoins" exists in the market).

of a bitcoin is projected to increase to about $2,000 in 2017.[108]

B. *Bitcoin: The Concept Explained*

Bitcoin at its most basic level is a type of electronic currency that is represented by computer code.[109] Bitcoin is not issued by any government, and is not backed by any physical commodity.[110] The only value a bitcoin has is the one attributed to it by the general public.[111] Furthermore, bitcoins are self-regulating due to their finite amount, and their inability to be copied and re-used.[112] The most defining feature of Bitcoin is that no central authority regulates their use.[113] Rather, all transactions run through a *peer-to-peer computer network* that does not maintain any personal identifying information of its users, which, in essence, renders Bitoin's transactions anonymous.[114]

1. The Bitcoin Exchange

The most basic definition of a peer-to-peer network, also referred to as "P2P network," is when "two or more [computers] are connected and share resources without going through a separate server computer."[115] In the case of Bitcoin, it is a more complex network "in which special protocols and applications set up direct relationships among users over the Internet."[116]

In order to access Bitcoin's peer-to-peer network, an individual must download the Bitcoin client software.[117] This program, commonly

108. *Id.*

109. Gerald P. Dwyer & Norbert J. Michel, *Bits and Pieces: The Digital World of Bitcoin Currency*, THE HERITAGE FOUNDATION (Sept. 16, 2015), http://www.heritage.org/research/reports/2015/09/bits-and-pieces-the-digital-world-of-bitcoin-currency.

110. *Id.*

111. *Id.*

112. *Id.*

113. *Id.*

114. *Id.* (discussing that: some critics claim that bitcoins are pseudo-anonymous because they can be linked back to an address. Specifically, that they can be linked back to the Internet address which the user used to connect to the Internet. In spite of this, bitcoin transactions are anonymous because of the fact that a Bitcoin transaction requires no sharing of personal information.); Furthermore, with some simple steps, an individual can protect his offline identity from is online presence. *How to Make Anonymous Payments with Bitcoin: A Step-by-Step Guide*, EXPRESSVPN, https://www.expressvpn.com/internet-privacy/bitcoin-anonymity/step-by-step-guide/.

115. James Cope, *Peer-to-Peer Network*, COMPUTERWORLD (Apr. 8, 2002, 1:00 AM), http://www.computerworld.com/article/2588287/networking/peer-to-peer-network.html.

116. *Id.*

117. Gerald P. Dwyer & Norbert J. Michel, *Bits and Pieces: The Digital World of Bitcoin Currency*, THE HERITAGE FOUNDATION (Sept. 16, 2015), http://www.heritage.org/research/reports/2015/09/bits-and-pieces-the-digital-world-of-bitcoin-currency.

referred to as the "wallet," connects the user through the Internet to the Bitcoin decentralized network.[118] This decentralized network provides the user access to a marketplace of sorts.[119] This marketplace is made up of all the other Bitcoin users.[120] Within this market the user can purchase bitcoins from the bitcoin exchange, purchase bitcoins from other users, sell bitcoins to other users, and even accept bitcoins as payment for goods or services.[121] However, in order to partake in any of these activities, the user must use their software generated mathematical linked keys—one public key and one private key.[122] These keys are used to verify the user's transactions and record the transactions on the Blockchain.[123] Without the use of these keys a Bitcoin transaction will not be registered as having ever occurred.[124]

### 2. The Bitcoin Blockchain

The Blockchain, essentially Bitcoin's only record-keeping device, is a "publically available database that record[s] every bitcoin transaction."[125] The Blockchain records every Bitcoin transaction by using the user's public key to register an entry in the database.[126] This entry does not have any identifying information other than the amounts exchanged.[127] Furthermore, the Blockchain is the only mechanism used to see what Bitcoins are in circulation.[128] In other words, "no bitcoins exist independently of the blockchain."[129]

The Blockchain, in simplest terms, has been described as a ledger.[130] If a transaction is not registered in the Blockchain, it is said to have never occurred.[131] In essence, the Blockchain acts as an authentication system.[132] It uses the user keys to authenticate the amounts being transferred, and authenticates that the user transactions actually took place.[133] Once the Blockchain has registered a transaction, the bitcoins in

118. *Id.* The "wallet" does not store Bitcoins, rather it acts more as a spreadsheet in the sense that it records a user's transactions. *Id.*

119. *See id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.*

129. *Id.*

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.*

a sense "exchange hands," and the user who made the initial transfer loses the right to use whatever amount of bitcoins was transferred.[134]

If a user loses their private key they will no longer have access to their bitcoins, and will essentially lose them forever.[135] On the other hand, if a thief obtains an individual private key, the thief can empty out that user account by transferring the user bitcoins to their own account.[136] In such a case, the user whose private key was stolen will permanently lose their bitcoins, and due to the nature of Bitcoin's anonymity, will not be able to retrieve the bitcoins despite their appearance in the Blockchain.[137]

### 3. Bitcoin: Example of a Transaction

For purposes of illustrating a typical Bitcoin transaction imagine that Kyle wants to transfer bitcoins to Hannah. First, Kyle, via the "wallet," must create a message that includes the address of where his bitcoins are being held so he can access them. This address will presumably be where Kyle wants his bitcoin funds to be withdrawn from. In addition to including his own address, Kyle must also include the address of the recipient. In this case, Kyle must include Hannah's recipient address.

Once this message is created, Kyle must sign the message using the private key provided to him by the Bitcoin software client. For purposes of verifying that Kyle indeed signed the message, Miners[138] then verify that Kyle indeed signed the message appropriately by using Kyle's public key. Upon completion of the above, Kyle broadcasts this transaction (message) to the Bitcoin network.

Once Kyle has broadcasted the transaction, Miners then need to verify that the address Kyle provided has the necessary funds to complete the transaction. Assuming that the address has the necessary funds, Miners then need to verify that the transaction is valid by checking Kyle's and Hannah's public keys.

If the transaction passes all these steps, and the Miners conclude that the transaction is valid, it is included in one "block" in the Blockchain. As soon as the transaction is included in the Blockchain, Kyle will no longer be able to spend the bitcoins associated with the address from which he transferred funds, and it is now Hannah who will be able to

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.* A "Miner" is an individual who uses his resources to authenticate transactions, and to verify that they are includible in the Blockchain. They usually have to verify transactions by "solv[ing] a computer resource-intensive computational problem built into the underlying Bitcoin protocol." Assuming Miners complete the transaction, they are rewarded with some combination of new bitcoins and transaction fees—which are typically paid for with bitcoins.

access them and have the ability to spend them.[139]

### C. *Bitcoin: The Legacy of Silk Road*

With the public's open acceptance of Bitcoin as a currency, its accessibility, and its most appealing trait the ability to keep transactions completely anonymous, it did not take long until savvy criminals began to use it as their currency of choice. In what has been deemed the most sophisticated Internet Black Market, the Silk Road was the greatest display of Bitcoin's ability to not only launder money and evade taxes, but to run a criminal enterprise with almost no formal physical ties.[140]

Silk Road was an Internet website that operated as a marketplace similar to that of Amazon.[141] The main difference between it and Amazon, however, was that instead of selling electronics, clothes, and sporting goods, Silk Road offered an avenue through which to sell bricks of cocaine, weapons, fake passports, and even provided contracting for illegal service providers (*e.g.*, forgers and hit men).[142] Although Silk Road was arguably run in the "dark web," which requires special steps in order to access it, it was not long until full manuals existed on what software was needed to access Silk Road, all while remaining anonymous in the process.[143]

The only currency that could be used on Silk Road was Bitcoin.[144] Despite Bitcoin's already anonymous nature, Silk Road ran an extra process to maintain the anonymity of purchasers and retailers.[145] Specifically, it used what is now termed a Bitcoin "Tumbler."[146]

In its simplest form, the act of "tumbling" involved sending one "transaction through a complex series of dummy transactions."[147] The purpose of this was to divide the transaction, the bitcoins involved in it, and the buyer and seller into various transactions in order to create layers that would hide the address from which the transactions originated.[148]

The Federal Bureau of Investigation (FBI) eventually caught wind of Silk Road despite its anonymous nature.[149] During the course of its 2012

139. *Id.*
140. Leger, *supra* note 7.
141. *Id.*
142. *Id.*
143. *See generally Guide on How to Access the Silk Road 3.0*, SILK ROAD DRUGS (Feb. 8, 2017), http://silkroaddrugs.org/guide-on-how-to-access-the-silk-road-3-0/ [hereinafter *Guide on How to Access the Silk Road 3.0*].
144. Leger, *supra* note 7.
145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*

investigation, the FBI caught a break and was able to access one of the servers that was sending and receiving Silk Road transactions.[150] From here, the FBI was able to target its administrator, presumed by most to be Silk Road's creator, Ross Ulbricht.[151] On or around October 1st 2012, the FBI arrested Ross Ulbricht in a San Francisco Public Library, and shut down Silk Road shortly thereafter.[152]

During Silk Road's short life, from around the beginning of 2011 until the end of 2012, it was estimated that approximately one million users had at one point used its services.[153] It was also estimated that nearly $1.2 billion in sales were made through Silk Road, all of which were made using strictly bitcoins as currency.[154] Ross Ulbricht had accumulated approximately 26,000 bitcoins from Silk Road transaction fees by the time of his arrest, which was then equivalent to approximately $4 million.[155]

Despite the arrests made by the FBI as a result of unveiling Silk Road, none of the arrests would have been possible without having access to Silk Road's internal structure.[156] Specifically, without access to Silk Road's inwards, the FBI would not have been able to dismantle the Bitcoin "tumbling" system used by Silk Road to preserve user identities.[157] It also would not have been able to locate the sources of messages because of Silk Road's use of the Onion Router, also known as "Tor," which was a software program that relayed computer messages through other computers on separate servers in order to disguise the messages' originating locations.[158] Lastly, even without both of these obstacles, the FBI still would not have been able to easily assess the Bitcoin owners involved in the Silk Road transactions because of Bitcoin's inherent anonymity features.[159]

## V. U.S. TREATMENT OF CRYPTO-CURRENCIES

With the prevalence of crypto-currencies, their development in the real world, and their real world value, interchangeable for legal tender, it is a wonder why they have not fallen under regulations typically used to regulate financial industries. This is especially true considering their

150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.*
154. *Id.*
155. *Id.*
156. *Id.*
157. *Id.*
158. *Id.*
159. *Id.*

ability to be abused, and their prevalence in criminal activity.

### A. *Department of the Treasury's Treatment of Crypto-Currencies*

Although crypto-currencies pose a very real threat to the stability of the economy, in part because of the disguising of income and financial transactions through anonymity, the U.S. Department of the Treasury, in a 2013 Guidance report by the Financial Crimes Enforcement Network, declared that crypto-currencies, and persons who regulate, exchange, reproduce, or otherwise use them, are not to be considered money service businesses (referred to as MSBs).[160] The implication is that individuals who administer, exchange or otherwise use crypto-currencies are not susceptible to the regulations laid out in the Bank Secrecy Act.[161]

The Bank Secrecy Act, also referred to as the "BAS," "is the primary U.S. anti-money laundering law."[162] The purpose of the Bank Secrecy Act is to help the United States combat money laundering by requiring that financial institutions maintain records of certain customers' transactions, and by requiring those institutions to report transactions that allude to circumstances in which an individual may have violated some type of criminal, tax, or regulatory statute.[163] Furthermore, the Bank Secrecy Act's most defining feature is its incorporation of the Money Laundering Control Act of 1986.[164]

The Money Laundering Control Act of 1986 made "money laundering a federal offense, forbid[] the structuring of currency transactions to avoid reporting by financial institutions, and require[d] financial institutions to develop a Bank Secrecy Act compliance program."[165] The compliance program, at a minimum, requires that money services businesses: (1) provide a system of internal controls that will ensure continued compliance with the Bank Secrecy and the Money Laundering Control Acts; (2) have an independent testing system for compliance; (3) the appointing of an individual who is trained to coordinate and monitor everyday compliance with the acts; and (4) implement a customer

---

160. DEP'T OF THE TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

161. *Id.* at 1.

162. DEP'T OF THE TREASURY, OFFICE OF THE COMPTROLLER OF THE CURRENCY, BSA AND RELATED REGULATIONS, https://www.occ.gov/topics/compliance-bsa/bsa/bsa-regulations/index-bsa-regulations.html (last visited Feb. 9, 2017). *See also* Jorge Mestre, *A Bribe New World: The Federal Government Gets Creative in Chasing Foreign Officials for Taking Bribes*, 26 U. FLA. J.L. & PUB. POL'Y 1, 2 (2015).

163. Bank Secrecy Act and Anti-Money Laundering Service, § 1.01 (2016).

164. *Id.*

165. *Id.*

identification program that is compliance with section 326 of the Patriot Act.[166]

Although these guidelines are set to ensure the reporting of various types of suspicious circumstances,[167] the pinnacle suspicious activity that requires the filing of a Financial Crimes Enforcement Network Form 112 Currency Transaction Report is any transaction which involves more than $10,000, or any set of transactions in one day that accumulate to more than $10,000.[168] The purpose of requiring the filing of these forms, and the recording of individuals' personal information, is to help authorities identify individuals who may be transferring money in an illegal manner.[169]

Despite the Bank Secrecy Act's resourcefulness in fighting money laundering, the Department of the Treasury's decision denouncing crypto-currencies and its users as being involved in money business services allowed all users of crypto-currencies to slide by the Bank Secrecy Act's compliance program unscathed. The consequence of this is that it left crypto-currencies largely unregulated.

Although the monetary consequences of leaving crypto-currencies unregulated are largely unknown, as evidenced by the reincarnation of Silk Road (first Silk Road 2.0, which was shut down, and now Silk Road 3.0 that is currently fully operable) the potential of abuse in using crypto-currencies to commit crimes is still very real.[170] Given the ongoing use of crypto-currencies, specifically Bitcoins, in the black market, it is concerning why a stronger stance to strip crypto-currencies anonymity,

---

166. DEP'T OF THE TREASURY, OFFICE OF THE COMPTROLLER OF THE CURRENCY, BSA AND RELATED REGULATIONS, https://www.occ.gov/topics/compliance-bsa/bsa/bsa-regulations/index-bsa-regulations.html (last visited Feb. 9, 2017).

167. *Id.*

> A Suspicious Activity Report filing is required for any potential crimes: 1. Involving insider abuse regardless of the dollar amount; 2. Where there is an identifiable suspect and the transaction involves $5,000 or more; and 3. Where there is no identifiable suspect and the transaction involves $25,000 or more. A SAR filing also is required in the case of suspicious activity that is indicative of potential money laundering or BSA violations and the transaction involves $5,000 or more.

*Id.*

168. 31 U.S.C. § 5313 (2016); *see* DEP'T OF THE TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN CURRENCY TRANSACTION REPORT (FINCEN CTR) ELECTRONIC FILING REQUIREMENTS 47 (July 2013), https://www.fincen.gov/sites/default/files/shared/FinCEN%20CTR%20ElectronicFilingInstructions%20-%20Stand%20Alone%20doc.Pdf#page=2.

169. *Id.*

170. *Guide on How to Access the Silk Road 3.0*, *supra* note 143.

and regulate their use, has not been taken considering their appeal to individuals interested in laundering money and avoiding taxes.

### B. *Internal Revenue Service's Treatment of Crypto-Currencies*

Unlike the Department of the Treasury's relaxed position on crypto-currencies, the IRS took a stronger stance in its goal to diminish the use of crypto-currencies to commit tax evasion.[171] In the IRS Notice 2014-21 publication, the IRS asserted that crypto-currencies were now considered property for purposes of income taxation.[172] This means that individuals will be held accountable for gains or losses they realize as a result of crypto-currencies exchanges or investments.[173] In most cases, they will be considered capital assets taxed at capital gains and losses rates.[174]

Although Notice 2014-21 now categorizes crypto-currencies as property under the current Internal Revenue Code, its applicability has been difficult to enforce because of the anonymous nature of crypto-currencies.[175] Because of the fact that the U.S. tax system requires voluntary reporting,[176] the reporting of crypto-currencies on an individual's income statement is completely up to that individual's discretion.[177]

In light of individuals' ability to hide income through the use of crypto-currencies, the IRS has made various demands to crypto-currencies exchanges in an attempt to have them disclose their user information.[178] This push to deteriorate crypto-currencies' anonymity comes after various investigations by the IRS into Bitcoin users that unveiled crypto-currencies' use to evade taxes.[179]

In sum, although the IRS has not had great success in stopping the use of crypto-currencies to evade taxes, and possibly facilitate money laundering, its codification of crypto-currencies has laid a foundation from which to control these faux currencies.

---

171. *Notice 2014-21*, INTERNAL REVENUE SERVICE 1, https://www.irs.gov/pub/irs-drop/n-14-21.pdf (last modified Mar. 25, 2014).

172. *Id.* at 1.

173. *Id.* at 3–4.

174. Subchapter P – Capital Gains and Losses, I.R.C. §§ 1201–98 (2016).

175. Nathaniel Popper, *Bitcoin Users Who Evade Taxes Are Sought by the I.R.S.*, N.Y. TIMES (Nov. 18, 2016), http://www.nytimes.com/2016/11/19/business/dealbook/irs-is-seeking-tax-evaders-who-use-bitcoin.html.

176. *See* discussion *supra* Part II.

177. Nathaniel Popper, *Bitcoin Users Who Evade Taxes Are Sought by the I.R.S.*, N.Y. TIMES (Nov. 18, 2016), http://www.nytimes.com/ 2016/11/19/business/dealbook/irs-is-seeking-tax-evaders-who-use-bitcoin.html.

178. Nicky Woolf, *Why the US Government Wants to Bring Cryptocurrency Out of the Shadows*, GUARDIAN (Nov. 27, 2016, 10:00 AM), https://www.theguardian.com/technology/ 2016/nov/27/coinbase-bitcoin-irs-government-summons-data-cryptocurrency.

179. *Id.*

## VI. PROPOSED SOLUTIONS

Having delved into the prevalence of money laundering and tax evasion both globally and in the United States, and the rise of crypto-currencies and their use in disguising real money, the question remains as to what steps can be taken to legitimize crypto-currencies, or at the very least, put an end to their use for illegal purposes. To decide how to put an end to these abuses it is imperative to look at how the United States investigates money laundering and tax evasion.

### A. *Investigation Methods*

In light of the financial consequences of money laundering and tax evasion,[180] the United States has taken affirmative action in trying to minimize their prevalence.[181] In order to combat money laundering and tax evasion simultaneously, the IRS performs a *financial investigation* on individuals suspected of committing either offense.[182]

A financial investigation, by its nature, is a document-intensive analysis of an individual's financial records.[183] This investigation is carried out by the IRS Criminal Investigation Unit, and consists of collecting an individual's financial statements, ranging from bank account records to motor vehicle records.[184] These documents, in theory, track the movement of money—also known as a "paper trail."[185] The purpose of establishing this "paper trail" is to determine where an individual's money is coming from—from whom, why, where it is being stored, and, in essence, whether it is evidence of any type of criminal activity.[186]

### B. *The Problem*

Due to the nature of financial investigations, one key element that is required for the IRS Criminal Investigation Unit to effectively perform its job is the existence of records of an individual's finances.[187] Thus, despite its best efforts to put a stop to money laundering and tax evasion, if financial records do not exist, there is simply no "paper trail" that can

180. *See* discussion *supra* Part III.

181. *See* discussion *supra* Part V.

182. INTERNAL REVENUE SERVICE, FINANCIAL INVESTIGATION – CRIMINAL INVESTIGATION (CI) (2016), https://www.irs.gov/uac/financial-investigations-criminal-investigation-ci.

183. *Id.*

184. *Id.*

185. *Id.*

186. *Id.* ("Tax evasion, public corruption, health care fraud, telemarketing and terrorist financing are just a few of the types of crime that revolve around money.").

187. *Id.*

be followed back to an individual committing either crime.[188]

Hence, the problem that arises for the IRS Criminal Investigation Unit's investigation of individuals committing money laundering and tax evasion offenses using crypto-currencies, specifically Bitcoin, is that crypto-currencies are anonymous.[189] As a result, no records of transactions are kept other than the Blockchain, which leaves no "paper-trail" for the IRS Criminal Investigation Unit to follow.[190]

Although the Blockchain is arguably a ledger, the issue with the Blockchain is that it does not link back to a physical individual.[191] Rather it only provides the Internet address where certain amounts of crypto-currencies are located.[192] The same issue arises here, which is that an individual can anonymously move both legally and illegally acquired crypto-currencies around the world, purchase goods and services with them, and even exchange them for legal tender. This is done all while avoiding taxes on the crypto-currencies, and in some cases, even laundering them into a commodity that can be reused in the real world without alerting the authorities.[193]

### C. *The Solutions*

Considering the complexity of cracking down on crypto-currencies, no simple answer exists for restricting their ability to launder money or evade taxes. However, building off avenues that already exist, the most feasible solutions seem to be to either acknowledge crypto-currencies as forms of international legal tender or create regulations that require crypto-currency exchanges to maintain identifying records of their customers.

#### 1. Recognition of Crypto-Currencies as Legal Tender

In theory, if the Department of the Treasury were to conclude that crypto-currencies should be considered a legal form of currency, and that users of crypto-currencies fall under the money services business definition, it would bring crypto-currencies under the Bank Secrecy Act's regulatory scheme. This would require crypto-currencies exchanges, or even individuals dealing in crypto-currencies, to create programs through which they will need to abide by the Bank Secrecy Act or face possible punishment.

---

188. *See* discussion *supra* Part V.A.
189. *See* discussion *supra* Part IV.
190. *See* discussion *supra* Part IV.B.2.
191. *See* discussion *supra* Part IV.B.2.
192. *See* discussion *supra* Part IV.B.2.
193. *See* discussion *supra* Part IV.

This solution would not only benefit United States law enforcement in combating money laundering, but would also benefit the IRS's efforts to stop tax evasion. Specifically, by requiring user crypto-currencies to abide by the Bank Secrecy Act any time one of the suspicious activities outlined in the Bank Secrecy Act occur, the IRS will be provided notice of the activity via Form 112.[194] The filing of Form 112, in combination with the Bank Secrecy Act's requirement that the appropriate records of customer's identities and transactions be kept,[195] will aid the IRS's efforts to appropriately conduct financial investigations on individuals who may be committing tax evasion, all while allowing the IRS to properly enforce Notice 2014-21.[196]

### 2. Require That Crypto-Currencies Exchanges Maintain User Identifications Records

In the alternative, the United States could promulgate laws that mandate crypto-currencies exchanges to require individuals to personally register, using personal identifying information, in order to use their services. Ideally, the loss of anonymity would lessen the appeal of crypto-currency.

This would hopefully discourage individuals from trying to launder money and evade taxes via crypto-currencies when they are fully aware that their online presence links back to their physical identity. Furthermore, requiring crypto-currencies exchanges to keep identifying information on their customers will facilitate the IRS's financial investigations into money laundering and tax evasion by creating a platform from which the IRS can trace online transactions. Lastly, it will aid the IRS in collecting taxes on crypto-currencies in accordance with Notice 2014-21 that may[197] have been misrepresented by an individual's voluntary disclosure of their crypto-currencies activities.

In sum, although either solution would be difficult to implement considering that both would require the cooperation of various government branches, in addition to crypto-currencies exchanges amendment of their rules, the idea behind both solutions is to do away with crypto-currencies' anonymous natures in order to discourage individuals from using them to launder money and evade taxes.

---

194. *See* discussion *supra* Part V.A.
195. *See* discussion *supra* Part V.A.
196. *See* discussion *supra* Part V.B.
197. *See* discussion *supra* Part V.B.

## VII. CONCLUSION

As evidenced by the various studies conducted by the United Nations and the United States, the consequences of money laundering and tax evasion costs the general public billions of dollars per year, which could be used for economic and social reform.[198] Although the United States has historically taken a rather strong stance in combating both of these criminal activities, it has taken a relaxed position on crypto-currencies in more recent years.[199] Although it is unknown just how significantly crypto-currencies contribute to money laundering and tax evasion, the reality is that they are a growing means by which individuals are able to successfully commit crimes while remaining undetected.[200] Considering the potential consequences of leaving crypto-currencies largely unregulated, it is time for the United States to reconsider the classification of this commodity and develop regulations through which it can regulate crypto-currencies transactions, or at the very least, identify individuals who are using crypto-currencies to launder money and evade taxes.

198. *See* discussion *supra* Part III.
199. *See* discussion *supra* Part V.
200. *See* discussion *supra* Part IV.