BITCOIN TRANSACTIONS: A BIT OF FINANCIAL PRIVACY[♦]

INTRODUCTION

Imagine going to a shopping mall today to buy a new television. When you get to the television store, you pick out the best television, and when the salesman scans your new purchase, you hand him or her some valuable jewels in exchange for the television. But wait, this is not how business transactions typically occur in 2016. However, if this were in 9000 B.C.,[1] when people bartered goods, it may have been plausible.[2] If you were in 600 B.C., when the first known "official" currency was created, then you could have paid with that currency.[3] If you were in 1661 A.D. then the notion of currency would have caught on, banks notes would have been printed, and businesses would readily

---

[1] This is with the understanding that it would not be a television at issue here, but rather something that would have been available for purchase or barter in 9000 B.C.

[2] *See* Rebecca Burn-Callander, *The History of Money: From Barter to Bitcoin*, TELEGRAPH (Oct. 20, 2014, 11:35 AM), http://www.telegraph.co.uk/finance/businessclub/money/11174013/The-history-of-money-from-barter-to-bitcoin.html.

[3] *See id.*

accept this method of payment in exchange for goods.[4] Almost 300 years later, in 1946, the first charge card was used; consumers no longer needed currency and could purchase items on a credit card.[5] Now, in 2016, you have the ability to pay with paper currency (i.e. cash), credit card,[6] mobile wallet applications[7] such as ApplePay[8] or Samsung Pay,[9] and Bitcoin.[10]

With the evolution in the way consumers transact business—from a barter system to a virtual currency system[11] such as Bitcoin—the need to regulate and monitor such transactions is vital. One can presume that in 9000 B.C. in a system of bartering, it would be important to know whether what one is exchanging is actually valuable and not fake.[12] When paper currency gained traction in the late 1600's and early 1700's,[13] there was a serious problem with the counterfeiting of bills in North Carolina.[14] Understandably, this apparent fraud and deception had serious negative effects on the economy.[15] In response, "[l]awmakers passed the first federal anti-counterfeiting laws in 1790, and since then Congress has regularly introduced new legislation as counterfeiting techniques have grown more sophisticated."[16] Similarly, laws against

---

[4] *See id.*

[5] *See id.*

[6] *See id.*

[7] Mobile wallet applications allow consumers to pay with a mobile device to which one has linked to a credit or debit card. *See, e.g.*, Dan Howley, *Samsung Pay vs Apple Pay vs Android Pay: Which Should Replace Your Wallet?*, YAHOO! TECH (Sept. 28, 2015), https://www.yahoo.com/tech/samsung-pay-vs-apple-pay-vs-android-pay-which-224028473.html ("[M]obile wallet apps . . . [are] . . . . [d]esigned to hold virtual versions of your credit . . . cards . . . [and] will eliminate the need for us to carry around traditional wallets.").

[8] *See id.* Apple Pay is a new payment system available on Apple's latest phone or watch, to which one can link a bank card. In order to pay for a purchase, a user must hold the linked device near a payment terminal and the linked device will allow you to choose which bank card the user wants to pay with. The phone will prompt each user through this process and confirm payment once it is done. *See* Lucy Warwick-Ching, *Apple Pay: What it Is and How it Works*, FINANCIAL TIMES (July 17, 2015, 2:15 PM), http://www.ft.com/cms/s/0/b1d97c44-2ad4-11e5-8613-e7aedbb7bdb7.html#axzz4FMhzKreS.

[9] Similar to ApplePay, Samsung describes its payment method in three steps. After linking a qualified bank card to your Samsung Pay phone application, a user selects the Samsung Pay icon, authorizes the payment by scanning one's finger on the home button, and lastly, by placing your phone near the in-store card reader to register the payment. *See Samsung Pay*, SAMSUNG, http://www.samsung.com/us/samsung-pay (last visited Sept. 16, 2016); *see also* Howley, *supra* note 7.

[10] *See* Burn-Callander, *supra* note 2.

[11] Throughout this Note, Bitcoin will be referred to specifically, however, all theories, facts, and conclusions generally apply to all virtual currencies. See Part I for an explanation on virtual currencies and the different types of virtual currencies available.

[12] One can imagine, for example, during ancient times, a person holding a jewel up to the light to see if the light passes through in order to determine the value of the jewel.

[13] *See* Neil Fulgham, *A Brief History of North Carolina Money*, U.N.C. U. LIBR., http://www2.lib.unc.edu/dc/money/ncmoney.html (last visited Nov. 18, 2015).

[14] *See id.*

[15] *See id.*

[16] Peter Followill, *Counterfeiting Laws and Penalties*, CRIMINAL DEFENSE LAWYER,

credit card fraud[17] and other types of money transfer systems[18] have been enacted over time as payment methods have evolved and changed from the 1600's to the present day.

Unlike a barter system, paper money, or credit cards, mobile wallet applications do not face issues such as counterfeiting. Rather, they utilize a consumer's bank account, credit card, or debit card, and simply provide an alternative way to use those particular preexisting methods of payment. Thus when it comes to fraud, a mobile wallet application such as ApplePay may have different concerns than a barter system, paper money, or credit cards since it simply utilizes the other methods of payment.[19] Additionally, the most recent payment system, Bitcoin,[20] is coming under significant scrutiny since it has been subject to certain issues that are both novel and unique by virtue of Bitcoin's status as a digital currency.[21] Like paper money and credit cards when they were first introduced to the market, issues[22] are arising and becoming more common with the increased use of Bitcoin. Since "[t]he Bitcoin system is private, with no traditional financial institutions involved in the transactions,"[23] there are different problems to consider that society has not faced in the past. Given that the U.S. legal system initially classified

---

http://www.criminaldefenselawyer.com/crime-penalties/federal/counterfeiting.htm (last visited Sept. 16, 2016).

[17] *See Credit Card Fraud*, CORNELL U. LAW SCH. LEGAL INFO. INST., https://www.law.cornell.edu/wex/credit_card_fraud (last visited Nov. 21, 2015).

[18] *See id.* (explaining that wire and bank transfers are the other types of money transfer systems for which fraud is a consideration).

[19] *See* Andrew Ross Sorkin, *Pointing Fingers in Apple Pay Fraud*, N.Y. TIMES (Mar. 16, 2015), http://www.nytimes.com/2015/03/17/business/banks-find-fraud-abounds-in-apple-pay.html?_r=0 (elaborating on the fact that so-called mobile wallet application fraud actually relates back to credit card fraud and/or the underlying payment method used to fund the mobile wallet application).

[20] *See* HISTORY OF BITCOIN, http://historyofbitcoin.org/ (last visited Nov. 18, 2015). Although Bitcoin is one of many virtual currencies, it is the most common and well-known form of virtual currency, *see id.* The development of Bitcoin started in 2007, and since then there has been no other form of virtual currency that has gained worldwide attention, *see id.*

[21] *See generally* Josh Hicks, *Government Increases Scrutiny of Bitcoin*, WASH. POST. (Aug. 13, 2013), https://www.washingtonpost.com/news/federal-eye/wp/2013/08/13/government-increases-scrutiny-of-bitcoin (analyzing the Senate Committee Hearings and the potential threats and problems with virtual currencies); Nate Raymond, *Accused Silk Road Creator Goes to Trial Amid U.S. Scrutiny of Bitcoin*, REUTERS (Jan. 12, 2015, 4:05 PM), http://www.reuters.com/article/2015/01/12/us-usa-bitcoin-trial-idUSKBN0KL0AW20150112 (discussing the United States' reaction to the use of virtual currency in drug trafficking and other crimes); Ryan Tracy, *Bitcoin Comes Under Senate Scrutiny*, WALL ST. J. (Nov. 5, 2013, 1:30 PM), http://blogs.wsj.com/washwire/2013/11/05/bitcoin-comes-under-senate-scrutiny (further analysis of the Senate Committee Hearings that will take place regarding policy issues raised by virtual currencies).

[22] *See* Daniel Cawrey, *The Five Biggest Threats Facing Bitcoin*, COINDESK (May 26, 2014, 5:33 PM), http://www.coindesk.com/five-biggest-threats-facing-bitcoin/; Ben Dyson, *Bitcoin's 3 Fatal Design Flaws*, POSITIVEMONEY (April 5, 2014), http://positivemoney.org/2014/04/bitcoins-fatal-design-flaws/.

[23] EDWARD V. MURPHY ET AL., CONG. RESEARCH SERV., R43339, BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 1 (2015) [hereinafter E. MURPHY].

Bitcoin as a currency,[24] then later as a commodity,[25] it is currently unclear which specific laws and regulations may apply to Bitcoin. However, what is certain is that regulation is forthcoming,[26] and arguably necessary, if Bitcoin is to become a more common method of payment and have an increased presence amongst U.S. financial institutions.[27]

If the use of Bitcoin, or any other form of virtual currency, does become more common amongst consumers, it will have significant disruptive potential with regard to transferring money between individuals and organizations. Recently, the U.S. Treasury Department[28] has expressed concern that "[t]errorism financiers may try to use virtual currencies such as Bitcoin to fund their operations as authorities crack down on the flow of illicit money through more traditional channels."[29] Furthermore, former U.S. Attorney General Eric Holder believes that "virtual currencies pose a challenge for law enforcement agencies, because they can be used to 'conceal illegal activity'" and to "buy drugs, weapons and other illegal goods and services."[30] This only scratches the surface of the many issues underlying Bitcoin, as can be seen with the Bitcoin exchange[31] Bitconica,[32] which was victim to a hack resulting in the theft of bitcoin valued at roughly $90,000.[33] Another example is Mt. Gox,[34] which launched in July 2010 and lost

---

[24] *See* Tanaya Macheel, *4 Court Cases Helping Shape the US Stance on Bitcoin*, COINDESK (Sept. 28 2014, 2:09 PM), http://www.coindesk.com/4-court-cases-helping-determine-us-stance-bitcoin/.

[25] *See* Pete Rizzo, *CFTC Ruling Defines Bitcoin and Digital Currencies as Commodities*, COINDESK (Sept 17, 2015, 10:06 PM), http://www.coindesk.com/cftc-ruling-defines-bitcoin-and-digital-currencies-as-commodities/.

[26] *See infra* Part II.

[27] *See infra* note 231.

[28] The U.S. Treasury Department is "responsible for . . . formulating and recommending economic, financial, tax, and fiscal policies, [and] serving as financial agent for the U.S. Government" among many other responsibilities. *See* U.S. DEPARTMENT OF TREASURY, https://www.treasury.gov/Pages/default.aspx (last visited Nov. 22, 2015).

[29] Kasia Klimasinska, *Terrorists Eyeing Bitcoin, Social Media to Fund Jihad, U.S. Says*, BLOOMBERG (June 12, 2015, 3:00 PM), http://www.bloomberg.com/news/articles/2015-06-12/terrorists-eyeing-bitcoin-social-media-to-fund-jihad-u-s-says.

[30] Evan Perez, *Holder: Bitcoin Raises Law Enforcement Concerns*, CNN MONEY (Apr. 8, 2014, 2:06 PM), http://money.cnn.com/2014/04/08/technology/bitcoin-holder/.

[31] *See What is Bitcoin?*, CNN MONEY, http://money.cnn.com/infographic/technology/what-is-bitcoin/ (last visited Sept. 7, 2016) (explaining that Bitcoin exchange is a marketplace that allows people to buy or sell bitcoin using different currencies).

[32] *See Bitcoinica*, BITCOINWIKI, https://en.bitcoin.it/wiki/Bitcoinica (last visited Nov. 18, 2015) (explaining that Bitcoinica was a Bitcoin exchange that suffered an internal security breach that resulted in a Bitcoin theft).

[33] *See* Tom Worstall, *Another Bitcoin Theft at Bitcoinica*, FORBES (May 15, 2012, 1:01 PM), http://www.forbes.com/sites/timworstall/2012/05/15/another-bitcoin-theft-at-bitconia/.

[34] *See* Yessi Bello Perez, *Mt Gox: The History of a Failed Bitcoin Exchange*, COINDESK (Aug. 4, 2015, 6:48 PM), http://www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange/. The failed Bitcoin exchange, Mt. Gox, was one of the world's first Bitcoin exchanges and accounted for up to eighty percent of Bitcoin trading volume during its peak, *see id.* Launching in 2010 and

$350 million in bitcoin almost four years later on February 25, 2014.[35] Four days after the hack, the Bitcoin exchange filed for bankruptcy and then a class action lawsuit was filed against Mt. Gox.[36] Currently, it is not possible to systematically monitor transactions and hold those accountable for the hack and theft, given the inherent privacy built into Bitcoin's technology.[37] The question then becomes, how do you hold Bitcoin exchanges responsible when it is so challenging to monitor transactions or hold hackers and thieves accountable? Are users of Bitcoin actually safe, and is their information secure?

To address these questions, this Note explores the existing framework of financial privacy laws and its application to Bitcoin and other virtual currencies. Whether Bitcoin by definition is a currency, commodity, or otherwise, financial privacy laws should arguably apply to protect users of Bitcoin, similar to the protection Bitconica and Mt. Gox needed in order to either prevent the theft of its money or somehow track the party responsible for the theft. Although Bitcoin, by definition,[38] may or may not be a currency, what is important is that it allows users to buy, sell, and exchange goods.[39] Rather than accepting paper money, credit cards, checks, or bank transfers, consumers can exchange Bitcoin[40] to complete certain financial transactions. As the use of Bitcoin becomes more popular,[41] users' financial privacy[42] should be taken into consideration as state and federal governments aim to regulate Bitcoin.[43] This Note proposes to identify and analyze the application of current financial privacy laws to the use of Bitcoin.[44]

Part I of this Note provides a general background on virtual currency with a focus on Bitcoin, what exactly Bitcoin is, and how it operates in the financial world today. Further, it explores the emerging regulatory framework aimed at controlling Bitcoin, and current case law arising out of the legal issues involving Bitcoin. Part II examines and evaluates current financial privacy laws as they apply to financial instruments and products, such as paper money and bank accounts. Furthermore, it identifies the underlying reasons and effects of financial

---

suspending operations in 2014, Mt. Gox was subject to a loss of $350 million, *see id.* Questions still exist whether the exchange was hacked or whether it was due to suspicious activity within the Bitcoin exchange, *see id.*

[35] *See id.*

[36] *See id.*

[37] *See infra* Part I.A.

[38] *See infra* Part I.A.

[39] *See infra* note 58.

[40] *See infra* Part I.A.

[41] *See* Richard Satran, *How Did Bitcoin Become a Real Currency?*, U.S. NEWS (May 15, 2013, 12:10 PM), http://money.usnews.com/money/personal-finance/articles/2013/05/15/how-did-bitcoin-become-a-real-currency.

[42] *See* discussion *infra* Part II.

[43] *See infra* Part I.B and Part I.C.

[44] *See infra* Part II.

privacy laws. Finally, this Note addresses the potential extension of current financial privacy laws to Bitcoin and the implications on virtual currency as a whole if it falls within the scope and consideration of financial privacy law.

I. VIRTUAL CURRENCY

The California Department of Business Oversight defines virtual currencies as "unique, typically encrypted, computer files that can be converted to or from a government-backed currency to purchase goods and services from merchants that accept virtual currencies."[45] Another definition by the Financial Action Task Force[46] (FATF) is that virtual currency is a "digital representation of value that can be digitally traded" and has many functions "but does not have legal tender status . . . in any jurisdiction."[47] Further, the FATF distinguishes virtual currency from fiat currency[48] or e-money[49] simply by the fact that fiat currency has legal tender status while virtual currency does not. Just as there are many types of fiat currencies,[50] there are a large number[51] of virtual currencies including, but not limited to, Litecoin,[52] Dogecoin,[53] Peercoin,[54] Darkcoin,[55] Primecoin,[56] and the most well-known, Bitcoin.[57] In exploring virtual currency, this Note will focus primarily on Bitcoin, and will provide a foundation for exploring the regulatory framework and financial privacy law considerations with regard to all virtual currencies.

---

[45] *What You Should Know About Virtual Currencies*, CAL. DEP'T OF BUS. OVERSIGHT (Apr. 2014), http://www.dbo.ca.gov/Consumers/Advisories/Virtual_Currencies_0414.pdf.

[46] *See* FINANCIAL ACTION TASK FORCE: VIRTUAL CURRENCIES, KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS 4 (June 2014), http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf ("The Financial Action Task Force is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.").

[47] *Id.*

[48] Fiat currency is real currency, real money, or national currency which is essentially paper money of a particular country. *See id.*

[49] E-money is a digital representation of fiat currency and has the same value as fiat currency and has legal tender status. *See id.*

[50] Each country's legal tender is considered fiat currency. Therefore, there are many difference types of fiat currencies including the US Dollar, Canadian Dollar, Euro, Pound, Yen, etc. *See id.*

[51] *See, e.g.*, Prableen Bajpai, *The 5 Most Important Virtual Currencies Other Than Bitcoin,* INVESTOPEDIA, http://www.investopedia.com/articles/investing/121014/5-most-important-virtual-currencies-other-bitcoin.asp (last visited Nov. 18, 2015).

[52] *See id.*

[53] *See id.*

[54] *See id.*

[55] *See id.*

[56] *See id.*

[57] *See id.*

A. *What is Bitcoin?*

Bitcoin is the first example of a category of digital currency known as cryptocurrency.[58] It was created in 2008 and released in 2009[59] and is not treated as conventional money, which is centralized and backed by the government.[60] Rather, Bitcoin is decentralized and based on mathematics.[61] This feature of not being issued by any central authority defines cryptocurrency. However, decentralization also contributes to Bitcoin's anonymity and makes it "well-suited for a host of nefarious activities such as money laundering and tax evasion."[62] Bitcoin is considered anonymous[63] since users can hold multiple addresses that are not linked to names or any personally identifiable information.[64] Almost to the contrary, however, transactions are also transparent since "[B]itcoin stores details of every single transaction that ever happened in the network in . . . a general ledger, called the blockchain."[65]

Bitcoin transactions involve high-level yet simple digital activities that account for elements of privacy, but also incorporate limited transparency. On a fundamental level, "[b]itcoin transactions are sent from and to electronic [B]itcoin wallets,[66] and are digitally signed for security."[67] These transactions are viewable to everyone on the network and the "history of a transaction can be traced back to the point where [B]itcoins were produced."[68] Additionally, it is important to note that bitcoins do not actually exist; there is nothing physical one can point to as a bitcoin.[69] Rather, it is more analogous to money held in a bank account that a bank account holder knows exists, but is not physically there.[70] When one wants to send bitcoins from his Bitcoin wallet to someone else, two things are needed: "a bitcoin address and a private key."[71] "A bitcoin address is generated randomly, and is . . . a sequence

---

[58] *See, e.g.*, *What is Bitcoin?*, COINDESK (last updated Mar. 20, 2015), http://www.coindesk.com/information/what-is-bitcoin/.

[59] *See id.*

[60] *See id.*

[61] For more on the mathematics behind Bitcoin see Eric Rykwalder, *The Man Behind Bitcoin*, COINDESK (Oct. 19, 2014), http://www.coindesk.com/math-behind-bitcoin/.

[62] *Cryptocurrency*, INVESTOPEDIA, http://www.investopedia.com/terms/c/cryptocurrency.asp (last visited Sept. 30, 2015).

[63] *Id.*

[64] *See infra* note 145.

[65] *What is Bitcoin?*, *supra* note 58.

[66] *See generally How to Store Your Bitcoins*, COINDESK, http://www.coindesk.com/information/how-to-store-your-bitcoins/ (last updated Oct. 19, 2015) ("Bitcoin wallets store the private keys that you need to access a bitcoin address and spend your funds.").

[67] *How do Bitcoin Transactions Work?*, COINDESK, http://www.coindesk.com/information/how-do-bitcoin-transactions-work/ (last updated Mar. 20, 2015).

[68] *Id.*

[69] *See id.*

[70] *See id.*

[71] *Id.*

of letters and numbers"[72] and can be thought of "as a safe deposit box with a glass front."[73] The private key is a secret sequence of letters and numbers and is able to "unlock [the safe deposit box] to take things out or put things in."[74] The point here is that since the safe deposit box has a glass front, presumably everyone knows what is inside—namely, how many bitcoins a particular user has in his Bitcoin wallet. However, one would need the private key in order to unlock it and take any bitcoins out or put any bitcoins in.[75] The concept of the glass front can be equated to revealing how much money one has in his bank account; in both instances, specific information is needed to access those funds.

When a user has the private key and is able to unlock his Bitcoin wallet, the transactions that occur from moving bitcoins in or out of the Bitcoin wallet are recorded on the blockchain.[76] The blockchain "is a public ledger of all [b]itcoin transactions that have ever been executed"[77] and "has complete information about the addresses and their balances right from the genesis block[78] to the most recently completed block."[79] In its simplest form, "the blockchain is like a full history of banking transactions"[80] and the "blocks . . . are like individual bank statements."[81] Additionally, "[b]ased on the Bitcoin protocol,[82] the blockchain database is shared" by all participating users in a system.[83] "The full copy of the blockchain has records of every [b]itcoin transaction ever executed"[84] and "can thus provide insight about facts like how much value belonged [to] a particular address at any point in the past."[85]

The idea that "[a] full transaction record of every [b]itcoin of every Bitcoin user's encrypted identity is maintained on the public ledger"[86]— also known as the blockchain—leads some to deduce that "[b]itcoin transactions are . . . pseudonymous, not anonymous."[87] In his legislative

---

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *See id.*

[76] To see a live blockchain, visit: https://blockchain.info/.

[77] *Blockchain*, INVESTOPEDIA, http://www.investopedia.com/terms/b/blockchain.asp (last visited Sept. 30, 2015).

[78] *See Genesis Block*, BITCOINWIKI, https://en.bitcoin.it/wiki/Genesis_block (last visited Nov. 21, 2015) ("A genesis block is the first block of a block chain.").

[79] *Blockchain*, *supra* note 77.

[80] *Id.*

[81] *Id.*

[82] Bitcoin protocol is the set of rules that make Bitcoin function. It establishes that only 21 million bitcoins can ever be created. However, these bitcoins can be further divided into smaller parts, the smallest being one hundred millionth of a bitcoin called a Satoshi. *See supra* note 58.

[83] *Blockchain, supra* note 77.

[84] *Id.*

[85] *Id.*

[86] E. MURPHY, *supra* note 23, at 3.

[87] *Id.*

report under the Congressional Research Service, Edward Murphy, along with his colleagues, noted that "[b]ecause of the public ledger, researchers have found that, using sophisticated computer analysis, transactions involving large quantities of [b]itcoin can be tracked."[88] Murphy further proclaimed that "if paired with current law enforcement tools it would be possible to gain a lot of information on the persons moving the [b]itcoins."[89] In addition, the legislative report notes that "if Bitcoin exchanges . . . are to be fully compliant with the bank secrecy regulations . . . required of other financial intermediaries, Bitcoin exchanges will be required to collect personal data on their customers . . . ."[90] As one considers Bitcoin's limited transparency, pseudonymous nature, and potential compliance with bank secrecy regulations, it is important to consider the current regulatory framework of Bitcoin.

B. *The Current Regulatory Framework of Bitcoin*

Since the creation of Bitcoin in 2009 by the infamous and anonymous Satoshi Nakamoto,[91] there have been numerous attempts to classify,[92] and thereby regulate, Bitcoin.[93] Most recently at the state level, on June 3, 2015, New York established a framework for regulating virtual currency businesses.[94] The New York State Department of Financial Services (NYSDFS) issued oversight regulations for virtual currency businesses operating in New York State.[95] New York State also "issued its first virtual currency license to a Bitcoin exchange" on May 7, 2015.[96] However, New York State did not stop there. NYSDFS also now requires businesses involved in a wide array of virtual currency transactions to be licensed.[97] The purpose of these regulations is to establish a base line standard for virtual currency businesses and to give NYSDFS the necessary authority to establish specific requirements to licensees.[98] California[99] and

---

88 *Id.*

89 *Id.*

90 *Id.*

91 *See Who is Satoshi Nakamoto?*, COINDESK http://www.coindesk.com/information/who-is-satoshi-nakamoto/ (last updated Feb. 19, 2016) (discussing speculation regarding the true identity of Satoshi Nakamoto, the creator of the Bitcoin protocol).

92 *See infra* Part I.C.

93 *See infra* Part I.C.

94 *See* E. MURPHY, *supra* note 23, at 14.

95 *Id.*

96 *Id.*

97 *Id.* at 15.

98 *Id.*

99 California has enacted legislation that allows virtual currency to be used to purchase goods and services, which repeals a provision of state law that only allowed lawful money of the U.S. Further, regulation of virtual currency businesses is under consideration by the California Department of Business Oversight. *See id.* at 16.

Connecticut[100] have also enacted legislation aimed at regulating Bitcoin.[101]

There is also activity at the federal level regarding Bitcoin regulation. The Senate Finance Committee[102] has directed other government committees to explore and review "any tax requirements and compliance risks implicated"[103] in [b]itcoin transactions. In this exploratory stage, these committees have contemplated how to classify virtual currency; is it "property, barter, foreign currency, or a financial instrument?"[104] Simply put, the classification assigned to Bitcoin,[105] may subject it to certain regulations while allowing it to evade others, either at the state or federal level. This seemingly arbitrary and inconsistent approach to the application of laws to Bitcoin—where different laws apply depending entirely on its classification—is illustrated through current case law.[106] In an effort to rein in Bitcoin, courts have attempted to articulate the contours of virtual currency in the eyes of the law and regulations.[107]

C. *The Current Case Law Shaping Bitcoin*

Current case law consists of seemingly inconsistent decisions focused on determining the nature of Bitcoin, thus subjecting it to regulation by different government agencies and laws. Most recently on September 17, 2015,[108] the U.S. Commodity Futures Trading Commission (CFTC) "confirmed that [B]itcoin and other digital currencies are commodities covered by the Commodity Exchange Act."[109] However, New York Law School professor Houman Shadab[110] believes that the CFTC's oversight of the technology should be limited to "the use of cryptographic technologies such as [B]itcoin for financial

---

[100] Similar to New York, Connecticut has enacted legislation requiring licenses for all virtual currency businesses. The legislation subjects these businesses to requirements imposed on money services businesses and new standards specifically for virtual currency businesses. Some of these new standards require a business to maintain a surety bond given the potential volatility of Bitcoin and possible risk of financial loss to consumers. *See id.* at 16–17.

[101] *See id.*

[102] *See id.* at 10 (noting this occurred in or around May 2013).

[103] *Id.*

[104] *Id.*

[105] *See infra* Part I.C.

[106] See *id.*

[107] *See id.*

[108] *See Release PR7231-15*, U.S. COMMODITY FUTURES TRADING COMM'N (Sept. 17, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7231-15.

[109] Rizzo, *supra* note 25.

[110] *See Houman B. Shadab*, NEW YORK LAW SCHOOL, http://www.nyls.edu/faculty/faculty-profiles/faculty_profiles/houman_shadab/ (last visited Nov. 22, 2015) ("Houman Shadab is a prolific and influential expert at the intersection of law, business, and technology. His research focuses on financial technology . . . and blockchains. . . . Professor Shadab has testified before the federal government . . . including before the [CFTC] on Bitcoin derivatives.").

derivatives."[111] Although Shadab believes that the ruling may have larger implications, he asserts that "[t]he action puts to rest any notion that virtual currencies qualify as securities"[112] since qualifying them as such would bring virtual currencies under the enforcement purview of the Securities and Exchange Commission (SEC). However, almost a year and a half earlier, in August 2013,[113] the SEC brought an action against Trendon Shavers, operator of Bitcoin Savings and Trust,[114] for "defrauding investors in [a] bitcoin Ponzi scheme."[115] In that case, a Texas judge "ruled that [B]itcoin is a currency or form of money,"[116] which then gave the SEC jurisdiction to pursue a case against Shavers and Bitcoin Savings and Trust.[117] The SEC charged Shavers and his illicit investment vehicle with "violating anti-fraud and registration provisions of security law"[118] but also made it clear that "this is not a bitcoin story, rather an all too common story of a scammer promising investors a too good to be true opportunity."[119] In response to this case, the SEC issued an investor alert[120] to warn "people about the dangers of investment scams using digital currencies such as [B]itcoin."[121]

Consider another case, *State of Florida v. Espinoza*,[122] in which Reid and Michell Abner Espinoza were arrested for engaging in fake transactions involving the conversion of $30,000 of cash into bitcoin.[123] Since these transactions exceeded the maximum threshold allowed under Florida state law, these individuals were charged under Florida's anti-money laundering law"[124] Although this case demonstrates a different approach from the instances previously discussed, since it utilizes anti-money laundering and unlicensed money transmission laws, it also raises another issue on appeal. On appeal, the defendants

---

[111] Rizzo, *supra* note 25.

[112] *Id.*

[113] *See* SEC v. Shavers, No. 4:13-CV-416, 2013 WL 4028182 (E.D. Tex. Aug. 6, 2013), http://www.law.du.edu/documents/corporate-governance/securities-matters/shavers/SEC-v-Shavers-No-4-13-CV-416-E-D-Tex-Sept-18-2014.pdf.

[114] Bitcoin Savings & Trust was an illicit investment vehicle used to defraud investors out of more than 700,000 bitcoins. *See* Emily Spaven, *SEC Charges Texas Man for Defrauding Investors in Bitcoin Ponzi Scheme*, COINDESK (July 23, 2013, 10:28 PM), http://www.coindesk.com/sec-charges-texan-man-for-defrauding-investors-in-bitcoin-ponzi-scheme; http://www.coindesk.com/bitcoin-ponzi-scheme-perpetrator-fined-40-million/.

[115] *Id.*

[116] Emily Spaven, *US Judge Rules Bitcoin 'is a Currency or Form of Money'*, COINDESK (Aug. 7, 2013, 1:41 PM), http://www.coindesk.com/us-judge-rules-bitcoin-is-a-currency-or-form-of-money/.

[117] *See id.*

[118] *Id.*

[119] *Id.*

[120] *See id.*

[121] *Id.*

[122] Florida v. Espinoza, No. F14-2923 (Fla. Cir. Ct. filed Feb. 2014); Florida v. Reid, No. F14-2935 (Fla. Cir. Ct. filed 2014).

[123] Macheel, *supra* note 24.

[124] *Id.*

filed to dismiss the money laundering charges[125] relying on the Internal Revenue Service (IRS) notice[126] that "bitcoin is not money,"[127] which would potentially undermine the state's ability to bring charges against them under Florida's anti-money laundering law. These additional issues regarding the conflict of the use of Florida's anti-money laundering law with the defendants' use of Bitcoin, and the IRS notice asserting that that Bitcoin is not money, illustrate the growing inconsistency regarding the classification and treatment of Bitcoin.

As previously discussed, conflicting reports and rulings give rise to significant inconsistencies in the application of law to Bitcoin—the one common component in the underlying transactions at issue. In one instance, the CFTC classified Bitcoin as a commodity; in another the SEC had jurisdiction because a judge ruled that Bitcoin is a currency; and in a third, the defendants used the IRS notice as a defense that bitcoin is not money.[128] One cannot help but think, was Bitcoin merely ruled a currency in *State of Florida v. Espinoza* in the pursuit of justice, to do what is right from a legal and societal perspective, but not necessarily supported by a consistent approach to current laws or regulations? What incentives do the CFTC and IRS have for giving it other classifications? Or is it the case that Bitcoin has different classifications depending on how it is used?

II. FINANCIAL PRIVACY LAW

In order to consider potential regulations surrounding the application of financial privacy laws to Bitcoin, it is necessary to understand and analyze the current legal framework of financial privacy as it applies to financial institutions and consumers. There are a number of financial privacy laws and regulations; exploring them will help address their scope as applied to the current financial framework and how they should, if at all, apply to virtual currency.

A. *Analyzing Current Financial Privacy Laws*

This Note will explore four major statutes that govern financial privacy today:[129] the Right to Financial Privacy,[130] the Gramm-Leach Bliley Act,[131] the Electronic Funds Transfer Act,[132] and the Bank

---

[125] *Id.*

[126] *See* I.R.S. Notice 14-21, 2014-16 I.R.B. 938.

[127] Macheel, *supra* note 24.

[128] *See* Release PR7231-15, U.S. COMMODITY FUTURES TRADING COMM'N (Sept. 17, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7231-15; SEC v. Shavers, No. 4:13-CV-416, 2013 WL 4028182 (E.D. Tex. Aug. 6, 2013); Florida v. Espinoza, No. F14-2923 (Fla. Cir. Ct. filed Feb. 2014); Florida v. Reid, No. F14-2935 (Fla. Cir. Ct. filed 2014).

[129] As of November 23, 2015.

[130] *See infra* Part II.A.1.

[131] *See infra* Part II.A.2.

Secrecy Act.[133] Although the foregoing in no way reflects an exhaustive list of the entire legal framework relating to financial privacy, it does provide a strong foundation upon which one can understand the basic infrastructure of the current system. Further, the following analysis will illustrate how these laws and regulations are aimed at protecting consumers' financial privacy, yet provide government regulators with access to financial data, allowing oversight in an effort to identify and prevent illegal and illicit activity.

1. Right to Financial Privacy Act

Currently, "[t]he United States has no general law of financial privacy."[134] At the federal level, the Right to Financial Privacy Act[135] (RFPA) "provides a measure of privacy protection by setting procedures for federal government access to customer financial records held by financial institutions."[136] However, there are state constitutions and laws that may provide greater protection.[137] Within the scope of the RFPA, the twin goals of financial privacy are apparent in the Act itself: one side being the protection of consumers' financial data, and the other side being the government's ability to access consumers' financial data in an effort to prevent illegal and illicit activities funded through various accounts of so-called bad actors.[138] As the Federal Reserve[139] notes in its Consumer Compliance Handbook, the RFPA "was enacted to provide . . . customers a reasonable amount of privacy from federal government scrutiny,"[140] thereby addressing the one side of financial privacy as it relates to consumers. However, the RFPA rightfully takes into account the other side of financial privacy and "establishes specific procedures that government authorities must follow when requesting a customer's financial records from . . . financial institution[s]."[141] This allows the government to access financial information through proper channels, if and when needed, such as when illegal or nefarious activities are suspected.

2. The Gramm-Leach Bliley Act

"The Gramm-Leach-Bliley Act . . . [(GLBA)] . . . requires

---

[132] *See infra* Part II.A.3.

[133] *See infra* Part II.A.4.

[134] M. MAUREEN MURPHY, CONG. RESEARCH SERV., RS20185, PRIVACY PROTECTION FOR CUSTOMER FINANCIAL INFORMATION 1 (2014) [hereinafter M. MURPHY].

[135] 12 U.S.C. §§ 3401–3422 (2010).

[136] M. MURPHY, *supra* note 134, at 1.

[137] *See id.*

[138] *See generally* Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2010).

[139] The Federal Reserve is the central banking system of the United States.

[140] FED. RES., RIGHT TO FINANCIAL PRIVACY ACT, CONSUMER COMPLIANCE HANDBOOK 1, http://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf.

[141] *Id.*

financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data."[142] It was enacted on November 12, 1999.[143] The GLBA establishes that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[144] Again, this addresses the side of financial privacy aimed at protecting consumers' financial data, specifically "nonpublic personal information" (NPI).[145] As it relates to consumers, NPI includes "personally identifiable financial information" consisting of, but not limited to, a customer's "name, address, income, Social Security number, . . . account numbers, payment history, loan, or deposit balances."[146] However, "NPI does not include information that [one has] reasonable basis to believe is 'publically available,'" which includes telephone numbers in a public directory or information distributed online or in paper media.[147] By establishing and acknowledging which information is NPI, financial institutions assure their customers that specific information will not be provided to third parties or other agencies without a proper or legally justifiable reason.

These legally justifiable reasons limit the extent to which the GLBA protects consumer privacy.[148] Section Fifteen of the GLBA lists exceptions that "apply to certain information-sharing, including disclosures for purposes of preventing fraud, responding to judicial process or a subpoena, or complying with federal, state, or local laws."[149] As seen with the RFPA, the GLBA also takes into consideration illegal and illicit activities. A consumer's financial data is protected, however, if the government or federal agency[150] finds reason to inquire about a particular consumer's financial information, the

---

[142] *Gramm-Leach-Bliley Act*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Nov. 19, 2015).

[143] *See S.900 – Gramm-Leech-Bliley Act*, CONGRESS.GOV, https://www.congress.gov/bill/106th-congress/senate-bill/900 (last visited Nov. 20, 2016).

[144] 15 U.S.C. § 6801(a) (2011).

[145] *How to Comply With the Privacy of Consumer Financial Information*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm (last visited Sept. 17, 2016).

[146] *Id.*

[147] *Id.*

[148] There are a number of exceptions listed in the GLBA, however, this Note only addresses specific exceptions directly related to the topic. *See id.*

[149] *Id.* There are additional exceptions under section thirteen, which apply to certain marketing activities but are part of the process in which financial institutions must disclose which information is considered NPI and which information is not considered NPI, *see id.* Even under section thirteen exceptions, NPI information is protected, *see id.*

[150] *See* discussion regarding FinCEN *infra* Part II.A.4.

government or agency is able to obtain that information. The government would be required to proceed through the proper legal channels, as required by the GLBA and other financial privacy laws, in order to obtain access to that information. In theory, such a system appears to be ideal where a consumer's financial data is protected until the government is able to provide legal justification[151] that allows it to bypass the wall of privacy established by the GLBA.

3. The Electronic Funds Transfer Act

The Electronic Funds Transfer Act (EFTA), which pre-dates the GLBA,[152] "describes the rights and liabilities of consumers . . . to have financial institutions identify the circumstances under which information concerning their accounts will be disclosed to third parties."[153] The EFTA, which Congress passed in 1978, "is intended to protect individual consumers engaging in electronic fund transfers . . . and remittance transfers."[154] The EFTA has since been amended numerous times to account for changes in the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank").[155] Although the EFTA in its original form had, and still has, the goal of helping protect consumers when they use electronic methods to manage their funds and finances,[156] Dodd-Frank further advanced that goal by addressing specifically the implications of the Financial Crisis of 2008.[157] As a result, Dodd-Frank essentially tipped the scale of financial privacy more towards the government since it aimed to "prevent the excessive risk-taking that led to the financial crisis"[158] and "provided common-sense protections for American families . . . ."[159] Although the changes implemented by Dodd-Frank were to protect consumers, they

---

[151] This is a threshold question not explored in this Note.

[152] *See* M. MURPHY, *supra* note 134.

[153] *Id.*

[154] FED. RES., ELECTRONIC FUNDS TRANSFER ACT, CONSUMER COMPLIANCE HANDBOOK 1, http://www.federalreserve.gov/boarddocs/supmanual/cch/efta.pdf.

[155] *See* H.R. 4173, 111th Cong. (2010) (enacted) (legislation aimed to promote financial stability by "improving accountability and transparency in the financial system . . . to protect consumers from abusive financial services practices . . .").

[156] *See* FED. RES., ELECTRONIC FUNDS TRANSFER ACT, http://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf.

[157] *See* Joel Havemenn, *The Financial Crisis of 2008: Year in Review 2008*, ENCYCLOPEDIA BRITANNICA, http://www.britannica.com/topic/Financial-Crisis-of-2008-The-1484264 (detailing the world economy in 2008 with the failure of banks, insurance companies, and mortgage lenders to name a few). One of the reasons for this severe economic recession was subprime mortgages which provided homes to families who could not afford them since reported financial data was never verified, *see id.* To prevent such systematic failure, Dodd-Frank and various other legislative measures put in place allow the government to regulate and oversee individual and corporate financial data, *see id.*

[158] *Wall Street Reform: The Dodd-Frank Act*, WHITE HOUSE, https://www.whitehouse.gov/economy/middle-class/dodd-frank-wall-street-reform.

[159] *Id.*

enable government oversight to much of the financial system in an effort to provide protection to consumers. One may question whether or not this was a clever way that the government has allowed itself to bypass the strict regulations that prevent it from readily accessing consumer financial data. When coupled with the Bank Secrecy Act,[160] the EFTA arguably has strong practical and justifiable considerations. It provides the government with the necessary tools to make inquiries into illegal, illicit, and nefarious activities, in a greater effort to link consumers with terrorism funding, and other activities of consideration to the U.S. government.

4. Bank Secrecy Act

Although many of the regulations discussed thus far have a significant impact on financial privacy, the Bank Secrecy Act[161] is the most directly related to the growing concerns[162] that Bitcoin needs to be regulated and more transparent[163] in order to prevent money laundering, the funding of terrorism, and other nefarious activities.[164] The Currency and Foreign Transactions Reporting Act of 1970—commonly referred to as the Bank Secrecy Act (BSA)—"requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering."[165] The BSA "requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 . . . and to report suspicious activity that may signify money laundering, tax evasion, or other criminal activities."[166]

Although these noted provisions are fairly simple, one of the more recent and noteworthy amendments to the BSA were made "to incorporate the provisions of the USA PATRIOT Act[167] which [require]

---

[160] *See infra* Part II.A.4.

[161] 31 U.S.C. § 5311 (2001).

[162] *See generally* Stan Higgins, *ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide*, COINDESK (July 7, 2014, 7:15 PM), http://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/ (discussing how terrorist organizations can potentially use virtual currency to fund their operations and go undetected), Stan Higgins, *US Treasury: Bitcoin's Use in Funding Terrorism 'Unclear,"* COINDESK, (June 12, 2015, 9:56 PM), http://www.coindesk.com/us-treasury-bitcoins-use-to-fund-terrorism-remains-unclear/ (analyzing reports by the U.S. Treasury Department that Bitcoin could be used to fund terrorism although it is unclear how certain that risk may be).

[163] *See* Peter J. Henning, *More Bitcoin Regulation Is Inevitable*, N.Y. TIMES (Feb. 2, 2014, 10:56 AM), http://dealbook.nytimes.com/2014/02/03/more-bitcoin-regulation-is-inevitable/?_r=0 (discussing regulations that have already been implemented and the notion that the government must look to current financial regulations in its effort to regulate bitcoin and other virtual currencies).

[164] *See* Higgins, *US Treasury*, *supra* note 162.

[165] *FinCEN's Mandate from Congress*, U.S. DEP'T. OF TREAS., http://www.fincen.gov/statutes_regs/bsa/ (last visited Sept. 7, 2016).

[166] *Id.*

[167] The USA PATRIOT Act was enacted by Congress to arm law enforcement with tools to help

every bank to adopt a customer identification program[168] as part of its BSA compliance program."[169] A financial institution's Customer Identification Program (CIP) "must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable."[170] Additionally, "[t]he procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer."[171] The CIP has a number of other provisions and establishes a variety of other guidelines and protocols[172] aimed at streamlining the process to ensure that the procedures in place are reasonable and practicable.[173]

These changes to the BSA, as mentioned briefly, were in response to the USA PATRIOT Act.[174] The Department of Justice notes that the USA PATRIOT Act was designed to "allow investigators to use tools . . . to investigate organized crime and drug trafficking."[175] Further, it "allows federal agents to follow sophisticated terrorists . . . , conduct investigations without tipping off terrorists . . . , [and] ask for a court order to obtain business records in national security terrorism cases."[176] In addition, the USA PATRIOT Act aims to facilitate information sharing among government agencies to help connect the dots[177] and help overhaul the law to reflect new technologies and threats.[178] These considerations provide significant context and reasoning for changes in the BSA. Although lawmakers have established significant financial privacy protections making it difficult for the government to access customers' financial data, the USA PATRIOT Act has allowed the government to readily bypass some of the regulations put into place by the RFPA, GLBA, EFTA, and the BSA. For example, under the USA PATRIOT Act, the government can bypass these regulations in instances in which it needs to actively fight terrorism and conduct investigations without informing people of

---

detect and prevent terrorism. See *Highlights of the USA PATRIOT Act*, DEP'T OF JUST., http://www.justice.gov/archive/ll/highlights.htm (last visited Sept. 17, 2016), for highlights of the USA PATRIOT Act.

[168] *See* Consumer Identification Programs for Banks, 31 C.F.R. § 1020.220 (2011).

[169] *See Bank Secrecy Act*, OFF. OF THE COMPTROLLER OF THE CURR., U.S. DEP'T OF TREAS., http://www.occ.treas.gov/topics/compliance-bsa/bsa/index-bsa.html (last visited Sept. 18, 2016).

[170] FINANCIAL CRIMES ENFORCEMENT NETWORK, TREASURY, *available at* http://www.gpo.gov/fdsys/pkg/CFR-2013-title31-vol3/pdf/CFR-2013-title31-vol3-sec1020-220.pdf.

[171] *Id.*

[172] Some of these provisions include guidelines on what customer information is required, exceptions for persons applying for a taxpayer identification number, and additional verification for certain customers. *See id.*

[173] *See id.*

[174] *Bank Secrecy Act, supra* note 169.

[175] *Highlights of the USA PATRIOT Act, supra* note 167.

[176] *Id.*

[177] *See id.*

[178] *See id.*

interest that they are being monitored.[179] Although this Note does not aim to analyze or evaluate the merits of the USA PATRIOT Act, the changes resulting from this Act as it relates to other regulations, such as the BSA, are noteworthy when evaluating overall financial privacy considerations, exceptions thereof, and the potential applicability to Bitcoin and other virtual currency.

In addition to the language of the laws and regulations itself, another point to note is that the BSA is administered by a branch of U.S. Treasury Department, the Financial Crimes Enforcement Network (FinCEN).[180] FinCEN has a number of duties and powers, which include:

> [m]aintaining a government-wide data access service . . . , [providing] analysis and dissemination of information in support of law enforcement investigatory professionals . . . , determin[ing] emerging trends and methods in money laundering and other financial crimes . . . , serv[ing] as the Financial Intelligence Unit of the [U.S.] . . . , [and] carry[ing] out other . . . regulatory responsibilities.[181]

Among FinCEN's enumerated duties, its responsibility to "determine emerging trends and methods in money laundering and other financial crimes"[182] seems to provide discretion as to what FinCEN should be targeting. The question here is whether Bitcoin falls under the category of emerging methods in money laundering and other financial crimes. If so, this may potentially subject Bitcoin to FinCEN's oversight given the duties and powers provided to FinCEN under the U.S. Treasury Department.

B. *Why Financial Privacy Laws Should Apply to Virtual Currency*

An all-too-common issue with Bitcoin involves understanding and defining what exactly Bitcoin is. One is able to understand what it does,[183] how it operates,[184] and have a basic idea of the legal framework aiming to regulate Bitcoin,[185] as well as recent case law[186] trying to apply existing laws to the use of Bitcoin. However, in all of this, there is one glaring inconsistency—is Bitcoin a commodity as defined by the CFTC?[187] Is it not money as defined by the IRS?[188] Or, is it money and

---

[179] *See id.*

[180] *See FinCEN's Mandate*, *supra* note 165.

[181] *Id.*

[182] *Id.*

[183] *See supra* Part I.A.

[184] *See id.*

[185] *See supra* Part I.B.

[186] *See supra* Part I.C.

[187] *See* Rizzo, *supra* note 25.

[188] *See* Macheel, *supra* note 24.

currency as determined by a judge and the SEC?[189] It appears that the legal system has defined Bitcoin as it sees fit in the pursuit of justice.

This pursuit of justice is demonstrated by the effort to hold Reid and Michell Abner Espinoza[190] accountable for fake transactions involving $30,000 of cash. This Note briefly explored *State of Florida v. Espinoza*[191] but will now go into a deeper analysis of the facts surrounding the case. With a transaction involving $30,000 in cash converted to bitcoins, one may assume that since the amount exceeds $10,000, the BSA gives ample latitude in making a legal inquiry into the transaction.[192] This inquiry would be justified under the BSA since the transaction exceeded $10,000 and would require a financial institution to file records of the transaction.[193] By filing transaction records, the government would then be able to review these transactions for questionable behavior and act accordingly as law enforcement mandates. In this case, the individuals were charged under a Florida State law[194] that embodies similar traits and goals as the BSA. However, when charged with a violation of this anti-money laundering law, the individuals tried to use an IRS notice, in which the IRS has claimed that Bitcoin is not money, as a defense.[195] One may argue that their claim has some ground, after all, the CFTC declared Bitcoin a commodity.[196] However, if the proper records were maintained, then the government would have been able to monitor these activities under the BSA and determine whether an investigation was necessary.

These inconsistencies bring out an important notion as it relates to cash. Fiat currency is treated differently when one physically holds it as cash or coins, when it is in a bank account and transferred to another account, and when it is converted to stocks, bonds, or other investment vehicles.[197] Can the same not be said about Bitcoin? When someone has cash and pays with cash, it is difficult to monitor those transactions[198] because there is no paper trail. If Consumer A has ten dollars in cash and pays Consumer B for some goods with that ten dollars in cash, there

---

[189] *See* Spaven, *supra* note 116.

[190] *See* Macheel, *supra* note 24.

[191] *See supra* Part I.C.

[192] *See supra* note 165.

[193] *See id.* The $10,000 threshold initiates separate processes that financial institutions must follow in order to abide by guidelines instituted by the BSA and other regulations aimed at preventing illegal, illicit, or nefarious activities, *see id.*

[194] *See* FLA. STAT. ANN. § 896.101(5)(a)–(b) (West 2016).

[195] *See* Macheel, *supra* note 24.

[196] *See* Rizzo, *supra* note 25.

[197] *See generally The Evolution of Money: Why Does Fiat Money Have Value?*, MONEY ENIGMA (May 5, 2015), http://www.themoneyenigma.com/the-evolution-of-money-why-does-fiat-money-have-value/.

[198] This is under the assumption that the consumer has received cash and is not accessing a financial institution to withdraw the money, therefore leaving no paper trail or record of the transaction.

may be no record of this transaction as far as financial institutions are concerned.[199] However, once this transaction is conducted with a bank check,[200] a credit card,[201] or other payment system,[202] it is more likely that there will be some record of the transaction.[203] It is only then, once a record is made, that some of the laws and regulations regarding financial privacy come into consideration. For example, if Consumer A paid Consumer B with $10,000 in cash, there is no record of that specific transaction.[204] But if that transaction occurred via credit card, the financial institution backing the credit card would be subject to keep a record of the transaction.[205] The same would apply to checks or cashier's checks, as is required under BSA guidelines.[206] It is not to say that just because a transaction exceeds a threshold amount, it insinuates illegal activities. However, it does flag the transaction,[207] enabling government agencies to conduct investigations into people or groups of people suspected of questionable activity.

The various provisions under the BSA and other laws and regulations allow the government to conduct these investigations. The RFPA, the GLBA, the EFTA, and the BSA all aim to protect consumer financial data thereby ensuring a high degree of financial privacy.[208] However, laws such as the BSA, as amended in response to the USA PATRIOT Act, require a CIP, which ensures that each account is verified and linked to a real, identifiable person.[209] There are a number of requirements, restrictions, and guidelines in place to ensure a reasonable and practicable effort[210] is made by each financial institution to gather this information. This allows financial institutions to flag certain transactions as the government mandates and, in turn, allows the

---

[199] This assertion is limited to comparisons involving alternative payment methods such as checks, credit cards, or cashier's checks—all which have some paper record and can be monitored by financial institutions and the government.

[200] A bank check is "a check drawn by a bank on its deposits in another bank." *Check*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/check#legalDictionary (last visited Aug. 24, 2016).

[201] "Using a credit card is like getting a loan . . . you're borrowing money until you pay it back later—either that month or over a period of months." *How Credit Cards Work*, CITIBANK, https://www.citicards.com/cards/wv/html/cm/student/faq/how-credit-cards-work.html (last visited Aug. 24, 2016). Usually credit cards are tied to financial institutions that fulfill your immediate financial obligation and allow you to delay your financial obligation until a later date, *see id.* As a result of these financial obligations, there are credit card applications to determine the worthiness of credit card users as well as recorded paperwork and documentation, *see id.*

[202] *See supra* Introduction (explaining the evolution of payment systems, thereby, noting some of the most common payment methods and systems used by consumers today).

[203] *See supra* Part II.A.4.

[204] *See supra* note 198.

[205] *See supra* Part II.A.4.

[206] *See supra* Part II.A.4.

[207] *See FinCEN's Mandate*, *supra* note 165.

[208] *See supra* Part II.A.

[209] *See supra* note 170.

[210] *See supra* note 172.

government to monitor the individual or individuals associated with the account.

Thus, with Bitcoin, the ability to have access to the customer information of each account must be made available. Bitcoin transactions worth ten dollars or $10,000 should be monitored by financial institutions in a similar manner to transactions involving a credit card or bank wire. Some may be quick to argue that this may infringe on an individual's right to privacy, but as Benjamin Charkow[211] asserted in his Note,[212] restrictions in the sharing of information as deemed in the GLBA "should extend only to the use and sharing of personally identifiable information with unauthorized persons."[213] Thus, if the government determines that it needs information regarding a certain [b]itcoin transaction, that information should be made available to aid the government in the necessary investigation.

Additionally, as Edward Murphy noted in his report, there are tools inherent in Bitcoin that will allow sophisticated users, such as government agencies, to monitor and track these transactions.[214] But what is vital in all of this is the collection of personally identifiable information, which Murphy notes[215] is needed to ensure full compliance with the BSA regulations required by financial intermediaries. Bitcoin enthusiasts may argue that there is transparency in the use of Bitcoin[216] because the history of each bitcoin is available for everyone to see;[217] a bitcoin can be traced to its creation;[218] and each [b]itcoin transaction can be traced back to its original owner.[219] However, the use of bitcoin does not include personally identifiable information. Although one can trace a bitcoin back to an address, there is no personally identifiable information associated with that address.[220] Even if sophisticated users are able to identify a user by his address, as Murphy suggests,[221] who is to say that that information is reliable or accurate? The laws and regulations described above require verified personal information for each account. If these same financial privacy laws apply to Bitcoin, then the reliability and accuracy of the identity of the user of each bitcoin address would increase significantly.

---

[211] Former law student at the Benjamin N. Cardozo School of Law, Yeshiva University, and author of *The Control Over the De-Identification of Data*.

[212] *See* Benjamin Charkow, *The Control Over the De-Identification of Data*, 21 CARDOZO ARTS & ENT. L.J. 195 (2003).

[213] *Id.* at 197.

[214] *See* E. MURPHY, *supra* note 23.

[215] *See id.*

[216] *See What Is Bitcoin?*, *supra* note 58.

[217] *See id.*

[218] *See id.*

[219] *See id.*

[220] *See* E. MURPHY, *supra* note 23, at 1.

[221] *See id.* at 3.

Alternately, active users of Bitcoin may assert that Bitcoin has protocols in place that allow for inherent financial privacy and that no further implementation of laws or regulations are needed. If one were to elaborate[222] on the inherent financial privacy that Bitcoin apparently affords,[223] one may assume that there are adequate privacy[224] measures in place. However, the Open Bitcoin Privacy Project[225] finds that "[f]inancial privacy is enforced lightly by the Bitcoin protocol."[226] The Bitcoin Wallet Privacy Rating Report,[227] released in Spring 2015, goes on further to assert that "[t]he short section on . . . [financial privacy] . . . dedicated by Satoshi in his whitepaper contains . . . suggestions, but no rules."[228] The problem with these suggestions is that they have largely been ignored due to the suspicious notion that Bitcoin is inherently anonymous.[229]

Despite Bitcoin's inherent privacy, which is still up for debate, the potential for Bitcoin to be integrated into the world's financial system is reason enough to ensure that additional financial privacy measures are initiated. It is essential that the U.S. government focus its efforts now at monitoring Bitcoin and virtual currency activities under the existing laws and regulations that monitor similar transactions involving checks, credit cards, and bank wire transfers. Monitoring [b]itcoin transactions has become more necessary than ever due to the growing interest in the use of virtual currency by financial institutions; recently, "BNP Paribas, Canadian Imperial Bank of Commerce, ING, MacQuarie and Wells Fargo . . . [became the] latest major financial institutions to partner with distributed ledger startup R3CEV."[230] With the addition of these institutions, R3CEV ("R3")[231] currently has a total of thirty financial

---

222 *See supra* notes 77–78, 82.

223 *See supra* Part I.A.

224 *See supra* Part I.A (discussing Bitcoin's characterization as anonymous or, more specifically, pseudonymous).

225 The Open Bitcoin Privacy Project is a global organization aimed at improving financial privacy within the Bitcoin ecosystem. The organization has studied and released reports on the numerous Bitcoin exchanges and the effectiveness that each has at protecting user privacy. *See* OPEN BITCOIN PRIVACY PROJECT, http://www.openbitcoinprivacyproject.org/ (last visited Aug. 25, 2016).

226 *Bitcoin Wallet Privacy Rating Report*, OPEN BITCOIN PRIVACY PROJECT (Spring 2015), https://bitcoinnewsmagazine.com/wp-content/uploads/2015/05/OBPP-Bitcoin-Wallet-Privacy-Rating-Report-Spring-2015.pdf.

227 The Bitcoin Wallet Privacy Rating Report highlights where software is successful in protecting privacy and where it is failing. It analyzes "behavioral patterns and features of Bitcoin software that measures its effectiveness at protecting the financial details of its users." *Id.* To see a more detailed explanation regarding the Privacy Ratings Methodology and Privacy Criteria Weighting, please see pages three and four of the report.

228 *Bitcoin Wallet*, *supra* note 226.

229 *See id.*

230 Pete Rizzo, *Wells Fargo, ING Among 5 New Banks Partnering with R3*, COINDESK (Nov. 19, 2015, 2:42 PM), http://www.coindesk.com/wells-fargo-ing-among-5-new-banks-partnering-with-r3/.

231 R3CEV founders envision bringing Bitcoin to financial institutions and engaged in a variety

institutions interested in the use of virtual currency, including Bank of America, BNY Mellon, Citi, HSBC, and Morgan Stanley.[232] R3 intends to develop "a blockchain or distributed ledger system tailored to the needs of the banking community and crafted with its input."[233] However, with the integration of these major financial institutions into the use of Bitcoin, it seems quite apparent that Bitcoin regulation is near, especially as it pertains to consumers' financial privacy. Regarding these financial institutions, a strict regulatory framework was put in place after the 2008 economic crisis. Therefore, the direct involvement of these banks and other financial institutions in the trading and other business dealings involving Bitcoin necessitates the application of the laws and regulations such as the RFPA, GLBA, EFTA, and the BSA.

CONCLUSION

Regardless, the notion that Bitcoin is intended to function as a decentralized currency[234] is not feasible long-term within the legal framework in the United States and around the world.[235] The right to financial privacy has evolved over time and has adapted to changes in the financial world. Currently, Bitcoin functions as a form of currency and commodity and, as a result, the right to financial privacy should adapt and be integrated into the use of Bitcoin. With a worldwide focus on terrorism and the funding thereof, the United States needs and requires the ability to monitor suspicious transactions. If individuals or groups of people are laundering money or using bitcoins to purchase illegal goods, the United States needs the ability to track these individuals. From a practical standpoint, Bitcoin needs to be regulated with regard to financial privacy considerations. From a legal standpoint, the many laws and regulations in place can and should apply to Bitcoin.

Sumit Agarwal∗

---

of projects including a peer-to-peer streaming network for the U.S. Treasury. *See* Stan Higgins, *Inside R3CEV's Plot to Bring Distributed Ledgers to Wall Street*, COINDESK (July 21, 2015, 9:05 PM), http://www.coindesk.com/r3cev-distributed-ledger-wall-street/.

[232] *See* Rizzo, *Wells Fargo*, *supra* note 230.

[233] *Id.*

[234] *See What Is Bitcoin?*, *supra* note 58.

[235] *See* Yessi Bello Perez, *European Union to Crack Down on Bitcoin After Paris Attacks*, COINDESK (Nov. 19, 2015, 12:30 PM), http://www.coindesk.com/european-union-to-crack-down-on-bitcoin-after-paris-attacks/ (discussing the European Union's intention to crackdown on bitcoin and aim to curb its potential terrorism financing).