

COUNTERING MONEY LAUNDERING AND TERRORIST FINANCING: A CASE FOR BITCOIN REGULATION

by
Emily Grace Fletcher

A research study submitted to Johns Hopkins University in conformity with the requirements for
the degree of Master of Global Security Studies

Baltimore, Maryland
May 2020

© 2020 Emily Fletcher
All Rights Reserved

ABSTRACT

Bitcoin was created in 2008 to serve as an alternative payment mechanism for the underbanked and unbanked, or those in regions where the formal financial system suffers from rampant corruption or ceases to exist altogether. However, criminals and terrorists quickly exploited Bitcoin's unique properties, namely its peer-to-peer nature and pseudo-anonymity, to facilitate extensive terrorist financing and money laundering schemes. Government reactions to safeguard national security interests have been extremely varied, ranging from outright bans to passive tolerance. This inconsistency stems from how to effectively classify Bitcoin. On one side are those who argue Bitcoin is a currency, and on the other are those who claim it is a type of asset. In the United States alone, these discrepancies have led to a bureaucratic turf war between different regulatory bodies, namely the Financial Crimes Enforcement Network, the Commodity Futures Trading Association, the Securities and Exchange Commission, and the Internal Revenue Service. This study seeks to move beyond the existing legal frameworks, arguing that Bitcoin should be classified as a technology and regulation should rest with private sector technology companies.

Primary Reader and Advisor: Sarah Clark

Secondary Readers: Jason Blazakis, Dr. Kimberley Thachuck

CONTENTS

Abstract	ii
List of Tables	v
List of Figures	vi
1 Introduction	1
2 Literature Review	4
2.1 Introduction	4
2.2 Properties of Bitcoin	4
2.3 Criminality Concerns of Bitcoin	7
2.4 Review of existing literature: Bitcoin as a currency	11
2.5 Review of existing literature: Bitcoin as an asset	11
2.6 Purpose of this study	13
3 Methods	15
4 Data	16
4.1 FinCEN: The BSA	16
4.1.1 Overview	16
4.1.2 Bitcoin properties covered	17
4.1.3 AML/CFT protections covered	20
4.2 The CFTC: The CEA	21
4.2.1 Overview	21
4.2.2 Bitcoin properties covered	23
4.2.3 AML/CFT protections covered	26
4.3 The SEC: Securities Act of 1933 and the SEA	27

4.3.1 Overview	27
4.3.2 Bitcoin properties covered	28
4.3.3 AML/CFT protections covered	30
4.4 IRS: 2014 Guidance	31
4.4.1 Overview	31
4.4.2 Bitcoin properties covered	32
4.4.3 AML/CFT protections covered	33
4.5 My Framework: Private Sector Self-Regulation	34
4.5.1 Overview	34
4.5.2 Bitcoin properties covered	39
4.5.3 AML/CFT protections covered	40
5 Discussion	46
6 Conclusion	48
References	50
Curriculum Vitae	60

LIST OF TABLES

1 Evaluating Regulatory Frameworks	45
--	----

LIST OF FIGURES

1	Trajectory of a Bitcoin Transaction.....	6
2	Illustration of the Bitcoin Mining and Verification Process	7
3	Comparison of Daily Fluctuations in the Price of Bitcoin	19
4	Fluctuations in Bitcoin Amidst the 2020 U.S.-Iran Conflict	24
5	Yearly Performance Comparison of Bitcoin and Other Safe Haven Assets Amidst the Outbreak of Novel Coronavirus	25
6	Flowchart for a Three-Tiered Framework for Bitcoin Regulation	37

CHAPTER 1: INTRODUCTION

Money is integral to the survival of terrorist groups. Without a consistent and reliable source of income, terrorist groups would not be able to maintain daily administrative tasks, support their members or carry out their attacks. In effect, terrorist groups would cease to “exist as organizations” altogether (Freeman 2011, 461). Because of the centrality of money, therefore, terrorist groups procure funding from a variety of legal and illegal sources, including from state sponsors, petty theft, illicit trade, extortion, charitable donations, and personal wealth (461).

Since the September 11 terrorist attacks, however, law enforcement agencies have established several effective counterterrorist finance methods for thwarting the movement of fiat currencies, or government-issued currencies, to terrorist groups. However, some argue the success of such counterterrorist finance programs may encourage terrorist groups to look elsewhere to finance their activities, namely the growing cryptocurrency market (Dion-Schwarz, Manheim, and Johnston 2019, 1-2). It is worth mentioning that while there are several hundred different types of cryptocurrencies, the focus of this paper will be primarily on Bitcoin.¹

Since Bitcoin was first created in 2008, its use has grown exponentially across the globe, bringing unprecedented benefits to individuals in societies where the formal banking sector is marred by corruption or, whether due to geographic location or systemic conflict, ceases to exist altogether. However, this widespread popularity has become a significant cause for concern for law enforcement officials and intelligence agencies worldwide.

The reasons are threefold. First, Bitcoin has a ‘pseudo-anonymous’ nature, meaning that while bitcoins can be traced to a certain computer in some instances or identified with a certain public key that is associated with a user, that user is never required to reveal his or her ‘real-

¹ This essay distinguishes between ‘Bitcoin’ (capitalized) – the technology and form of cryptocurrency, and ‘bitcoin’ (uncapitalized) – the individual units of the cryptocurrency.

world' identity. Second, Bitcoin was designed as a peer-to-peer platform so as to bypass the regulatory instruments of a state's traditional financial sector. Third, the nature of Bitcoin transactions makes them transnational, near instantaneous, and irreversible. These points taken together – plus the fact that the creation and use of new cryptocurrencies has outpaced policy, regulation, and law enforcement initiatives – have enabled terrorist organizations and organized crime syndicates to abuse the Bitcoin system for terrorist financing, money laundering, and other criminal activities.

Consequently, several regulatory bodies in the United States (U.S.) have endeavored to establish regulatory jurisdiction over Bitcoin transactions, namely the Financial Crimes Enforcement Network (FinCEN), the Commodity Futures Trading Commission (CFTC), the Securities and Exchange Commission (SEC), and the Internal Revenue Service (IRS). All four entities view Bitcoin differently and have attempted to regulate Bitcoin accordingly, by imposing their relevant legal frameworks.

For example, FinCEN views Bitcoin as a currency and has determined regulation according to the Bank Secrecy Act (BSA). The CFTC regards Bitcoin as a commodity, citing the Commodities Exchange Act (CEA) as the appropriate regulatory framework. The SEC considers Bitcoin to be a type of security and advocates regulation under the Securities Act of 1933 and the Securities Exchange Act (SEA). Finally, the IRS issued a Guidance in 2014 determining that Bitcoin is a property for federal tax purposes.

Although there is merit to each argument, Bitcoin was ultimately created to purposely avoid regulation by formal financial institutions. As such, none of the perspectives or regulatory frameworks proposed by FinCEN, the CFTC, the SEC, and the IRS truly account for the unique properties of Bitcoin as well as users' interests in a secure system of transactions that is safe

from the purview of government entities. In addition, these competing narratives have led to a bureaucratic turf war over regulation, making transacting in Bitcoin extremely confusing for users. Moreover, these competing regulations threaten over-regulation, which may push users to seek illicit means to use Bitcoin and escape regulation altogether.

To avoid these issues, I argue that Bitcoin should be classified as a technology with financial components, and regulation should rest with private sector technology companies, namely an international association known as the World Wide Web Consortium (W3C). I propose a three-tiered framework for regulation: at the bottom in the first tier are individual users who are regulated by the second tier, which is composed of companies offering services in Bitcoin such as buying, selling, exchanging, or storing bitcoins in a wallet. These Bitcoin companies are regulated by the third tier, represented by the W3C. The W3C acts in accordance with state governments and Bitcoin companies to establish certain standards for the community of Bitcoin users. To truly counter terrorist financing and money laundering with Bitcoin, and to effectively protect national security interests, regulation must be transnational in nature and bottom-up, not imposed from above and top-down.

CHAPTER 2: LITERATURE REVIEW

Introduction

Since the creation of the Internet in the early 1980s, everyday objects and transactions have become increasingly digitized, with impacts permeating virtually all sectors of human life including the military, communication, healthcare, infrastructure, energy, and financial divisions. The financial sector has been impacted by the advent of intangible, ‘digital’ currencies as an alternative to traditional, tangible fiat money, which is a government-issued paper currency that largely replaced the gold standard system.

Digital currencies, also known as cryptocurrencies, come in two main forms: centralized or decentralized/distributed. Examples of the former include ‘loyalty points’ from retail companies or ‘air miles’; they are confined within the centralized structure of a particular entity (Nian and Chuen 2015, 7). Decentralized digital currencies, on the other hand, can be used in transactions inside and outside of a network, facilitated by the use of readily and widely accessible open-source software. Examples include Litecoin, Dogecoin, and Bitcoin. Since first proposed by creator Satoshi Nakamoto in 2008, Bitcoin has gained significant publicity as the world’s first decentralized cryptocurrency and the current leader of the cryptocurrency market (Corbet et al. 2019, 182).

Properties of Bitcoin

Nakamoto designed Bitcoin to be “an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other” (Nakamoto 2008, 1). This direct peer-to-peer (P2P) nature of the Bitcoin system discounts the need for third parties, such as a central bank or another regulatory entity, to facilitate and validate transactions. Bitcoin operates on a fully decentralized and distributed open-source software

platform, meaning that not only can anyone access it, but also each user is connected to each other in the network and can leave or enter the network at any time (Nian and Chuen 2015, 11-12).

Important components of the Bitcoin system include: bitcoins, wallets, public and private keys, and the blockchain. The coins themselves are not tangible, rather they are composed of lines of code. Each user has a wallet to store his or her bitcoins. These wallets give the user an address, “akin to a bank account number”, and therefore also a pseudo-identity, however a user is rarely required to disclose his or her real-world identity when obtaining a wallet, rather what information is required can usually be “fabricated” (Nian and Chuen 2015, 15; Bollen 2013, 6; La Huis and McKeown, 2017, p. 5). For example, only an email address is required to obtain certain digital wallets. Payments are made by directing transactions to the address of a wallet (Bollen 2013, 6).

Each wallet, and therefore each user, is connected to a public and private key. The public key, as the name suggests, is made available to the entire network and is used “to generate Bitcoin addresses, sign transactions, and verify payments” (Nian and Chuen 2015, 21). In other words, the public key is “the Bitcoin address to and from which payments are sent” and it is used to verify signatures of transactions that are signed with the private key (21). It is possible to derive a public key from a private key but not vice versa, so it is extremely important that private keys be stored securely in the wallet (21). The user that controls the keys associated with the bitcoin is the only person able to transfer the bitcoin; loss of the keys means the bitcoins are no longer accessible (Bollen 2013, 7). Figure 1 depicts how a bitcoin transaction works using the public and private keys (Nakamoto 2008, 2).

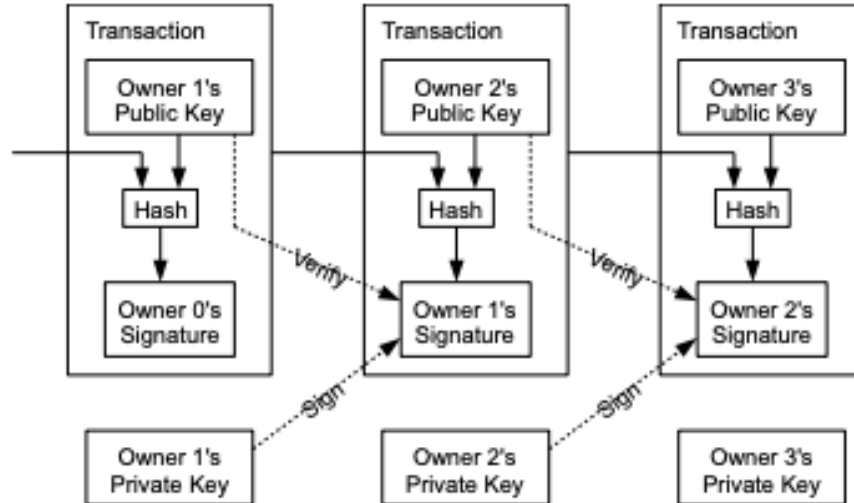


Figure 1: Trajectory of a Bitcoin Transaction

Finally, the blockchain is a public list on which each transaction is recorded. All records include the public keys of both the sender and the recipient, as well as the amount transacted and the time that the transaction occurred (Nian and Chuen 2015, 22).

At the time of writing, there are three main ways users can acquire bitcoins: through an online purchase or from a Bitcoin vending machine, in exchange for goods and services, or through mining (Volastro 2014). Mining is the process by which ‘miners’ solve complex mathematical problems to process transactions, which are then added to the blockchain after it is determined by a consensus that the transaction is valid (Nian and Chuen 2015, 19-20). In this way, miners – not a third party such as a central bank or other regulatory entity – are responsible for updating, maintaining, and verifying transactions on the blockchain. Figure 2 depicts the mining and verification processes (Uhl et al. 2018, 11).

Illustration of Bitcoin

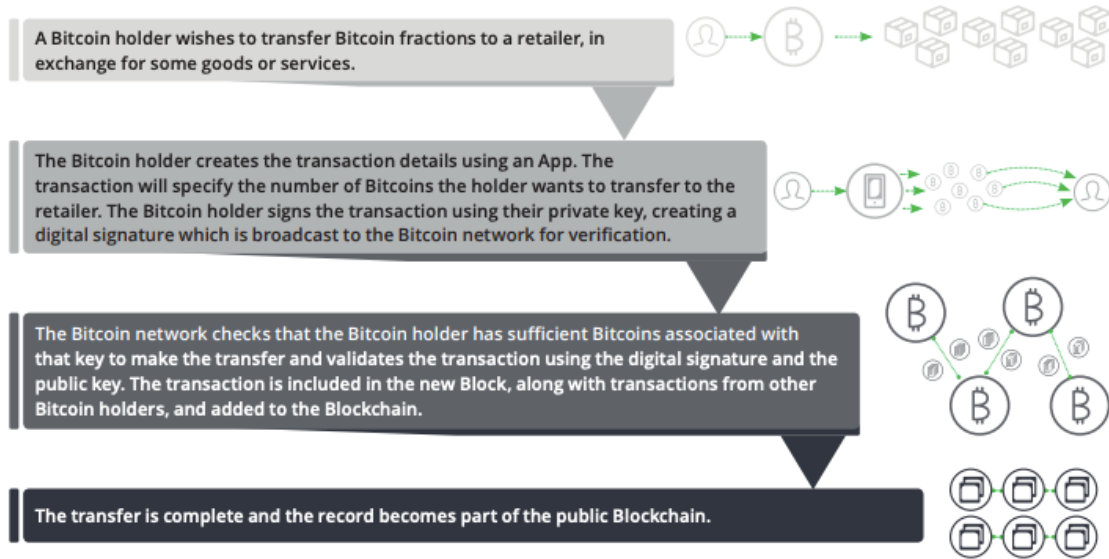


Figure 2: Illustration of the Bitcoin Mining and Verification Process

In addition to operating independently of a central authority such as a central bank, Bitcoin is also not linked to a commodity like gold. Consequently, the value of bitcoins is derived from users' trust and confidence in the system and its algorithms (Chu, Nadarajah, and Chan 2015, 2; Uhl et al. 2018, 9).

Owing to these properties, Bitcoin has ushered in a new transformative era in global banking. However, it has also caught the attention of law enforcement officials and intelligence agencies for its potential use in money laundering, terrorist financing, and other criminal activities.

Criminality concerns of Bitcoin

There are several qualities to Bitcoin that make it attractive to criminals. First, Bitcoin is 'pseudo-anonymous'; certain identifying information can be gleaned from the system, but not anything explicit. For example, the publication of a users' public keys on the blockchain means that transactions "to and from any Bitcoin address can be traced" to a source (Nian and Chuen 2015, 22). Moreover, the amount and time of the transaction may reveal important information

about habits or patterns unique to the parties involved. A wallet can also be tied to the specific Internet Protocol address of a user's device. Despite this, users are almost never required to disclose their real-world identities, which may present a huge incentive for potential criminals.

Second, the P2P nature of transactions can enable the financing of terrorist groups, as Bitcoin transactions need not pass through “the regulatory controls that third-party institutions... are legally bound to perform” (Reynolds and Irwin 2017, 173). Third, and related, Bitcoin is attractive due to the “global reach and speed” of transactions (La Huis and McKeown 2017, 5). This is partly due to the fact that transactions are not subject to regulatory oversight, but it is also due to the nature of the technology itself. Transactions can be “conducted nearly instantaneously and across many borders”, which may prove advantageous for terrorist groups who may want “to quickly move illicit funds to and from a wide variety of places around the world” (5). It also reduces the time horizons law enforcement agencies have to detect and intercept suspicious payments (Brill and Keene 2014, 14).

Fourth, Bitcoin is attractive for its relative ease and low cost of use (Brill and Keene 2014, 14). Using Bitcoin arguably requires very little technical skill, and the only materials needed are devices that can be connected to the Internet (La Huis and McKeown 2017, 5; Brill and Keene 2014, 14). In this way, transferring bitcoins can be as easy as sending an email.

Finally, the fact that payments are irreversible may be attractive to terrorist groups (Brill and Keene 2014, 7). There is no additional verification needed to finalize a payment, which enables transactions to be processed more quickly (14). Moreover, once the money is sent it cannot be reversed, which is logically important for terrorist groups that remain extremely dependent on reliable financial contributions (14).

Despite this discussion, some experts doubt the utility of Bitcoin in terrorist financing or money laundering schemes. After conducting semi-structured interviews with subject matter experts, Carroll and Windle (2018) concluded that there is simply not enough empirical data to demonstrate that terrorists and criminals are using Bitcoin to meaningfully enhance revenues. They argue Bitcoin is still too new and underdeveloped of a system; terrorists prefer instead to stick to trusted methods of generating and moving money using traditional cash, *hawala* systems, and the drug trade. In a similar vein, Dion-Schwarz, Manheim, and Johnston (2019) contend that the money raised by terrorists and criminals through Bitcoin comprises a negligible portion of their revenues. Related, Goldman et al. (2017) determined that instances where terrorists and criminals use Bitcoin are purely “anecdotal” and not representative of a growing trend (2).

The other side of the debate houses figures such as Yaya Fanusie, former economic and counterterrorist finance analyst with the Central Intelligence Agency. Fanusie (2019) uncovered the first identifiable instance of terrorists using Bitcoin and has warned that, on the contrary, terrorist groups and criminal organizations have started to depend more readily on Bitcoin, as their more traditional sources of financing have suffered more frequent disruptions from law enforcement in recent years. To justify these arguments, Fanusie and other experts have highlighted the growing number of cases involving terrorists, criminals, or individuals sympathetic to their causes.

Prominent instances include a 2018 report from Europol in which the organization estimated that in Europe, criminals were using cryptocurrencies including Bitcoin to facilitate the money laundering of “as much as \$5.5 billion (£4 billion) in illegal money” (Corcoran 2018). More recently, in 2020 American citizen Zoobia Shahnaz was dealt a 13-year prison sentence in

the U.S. for funneling \$150,000 in Bitcoin to the Islamic State (U.S. Department of Justice 2020).

In yet another example, Hamas has reportedly developed an algorithm that creates new Bitcoin donation addresses or a new Bitcoin wallet for each donor (Smith 2019; Liv 2019, 5-6). Through this campaign, members send Bitcoin addresses to potential donors, for example, who can then directly transfer money to Hamas (Azani and Liv 2018, 4). Consequently, it is estimated that in less than one month (between March 29 and April 16, 2019), Hamas raised 0.6 bitcoin – approximately \$3,300 – through “website-created wallets” (Wilson and Williams 2019). Fanusie (2019) argues that this objectively small amount of money is not indicative of its importance. Terrorism is a notoriously cheap enterprise; the September 11 terrorist attacks – the pinnacle of attacks to date, being the deadliest and most sophisticated – allegedly cost al-Qaeda only \$500,000 to execute but produced approximately \$3.3 trillion dollars in damages (Carter and Cox 2011). In other words, for every dollar al-Qaeda spent, it cost the U.S. \$7 million (Carter and Cox 2011).

In light of these revelations, this paper takes the stance that Bitcoin can and does facilitate terrorist financing and money laundering. An added concern for law enforcement officials and policymakers is that the creation and use of new cryptocurrencies has proliferated exponentially in recent years, outpacing policy and regulation. The need to devise appropriate regulatory strategies is exacerbated by the fact that Bitcoin was designed explicitly to avoid traditional regulatory measures. This has led to a literary explosion concerning how best to classify and regulate Bitcoin. Most of the existing literature can be split into two camps: Bitcoin should be classified as a currency versus as an asset.

Review of existing literature: Bitcoin as a currency

Most of the early literature (for example Kaplanov 2012) on Bitcoin classification argues it should be treated as a new type of digital or virtual currency, alternative to traditional government-backed fiat currencies. Turpin (2014) notes that Bitcoin is essentially the digital equivalent of cash, while McCallum (2015) presents the argument that there has been a historical trend towards electronic and digital banking; Bitcoin is simply the latest evolutionary step of the development. Grinberg (2011) cites the acceptance of the Iraqi Swiss dinar to defend against the popular criticism that Bitcoin cannot be considered a currency because it is not backed by a government nor tied to a commodity. Wiseman (2016) criticized the IRS' 2014 decision to classify Bitcoin as a property for tax purposes, asserting that a market analysis demonstrates that most users are treating Bitcoin as a currency. Schilling and Uhlig (2019) create a model that demonstrates Bitcoin can compete as a viable alternative to traditional fiat currencies in the current monetary system, whereas Carrick (2016) assesses that Bitcoin serves as a viable complement to other currencies.

If Bitcoin is to be classified as a currency, the corresponding legal framework that would dictate the terms of its regulation is the BSA, and the body responsible for overseeing this regulation would be FinCEN, which is located within the U.S. Department of the Treasury. This is significant, as FinCEN (2013) has declared that Bitcoin exchangers and administrators would be classified as Money Services Businesses (MSBs) and therefore are subject to strict reporting and registration requirements.

Review of existing literature: Bitcoin as an asset

The literature within this category is much less straightforward and divided into many subsections according to different types of assets. Yermack (2013); Dorfman (2017); Colville

(2014); and Claeys, Demertzis, and Efstathiou (2018) argue that Bitcoin should be conceptualized more as some sort of ‘speculative asset’, as users exploit the volatile price fluctuations with a view towards maximizing profits. Both Glaser et al. (2014) and Baur, Hong, and Lee (2015) conduct studies analyzing the behavior and intentions of users by looking at trading and transaction data on the blockchain, ultimately determining that the majority of holders primarily use Bitcoin as an asset for investment.

Others argue that Bitcoin should be treated like a commodity. Gronwald (2019) compared the Bitcoin market to those of crude oil and gold to demonstrate that Bitcoin functions most like a commodity, whereas Shahzad et al. (2019) discuss the viability of bitcoin as a safe haven asset in comparison to other commodities like gold. Prentis (2015) and Mandjee (2015) contend that Bitcoin fits into the definition outlined by the CEA, citing the law’s “and all other goods and articles” specification (Commodity Exchange Act of 1936). This aligns with the CFTC’s 2015 ruling that Bitcoin should be considered a commodity. If true, this would mean that the legal framework most appropriate to regulate Bitcoin transactions would be the CEA, and the body responsible for the regulation would be the CFTC.

Still others claim that Bitcoin should be classified as a security. Yang (2013) and Swartz (2014) argue that the definitions of a security outlined in the Securities Act of 1933 and the SEA are broad enough to include Bitcoin so long as it can be conceptualized as an investment contract. Lyandres, Palazzo, and Rabetti (2019) conclude that regulations for Initial Public Offerings (IPOs) can be applied to Initial Coin Offerings (ICOs) in Bitcoin and thus Bitcoin should be regulated as a security. If deemed a security, the entity responsible for Bitcoin regulation would be the SEC, with the aforementioned two laws imposing several regulatory and reporting requirements. However, the SEC has taken a contextual and *ad hoc* approach to

classifying Bitcoin, arguing that regulation will depend on the nature and purpose of the Bitcoin transaction or ICO.

Another branch of literature suggests that Bitcoin should be classified as a type of property. Low and Teo (2017) and Fox (2019) support this claim, citing private law rights. Chason (2019) argues that Bitcoin transactions resemble real estate property transactions. The IRS (2014) determined that Bitcoin should be considered a property for federal tax purposes. Roman (2015) outlines extensively the repercussions for users arising from this framework of regulation.

Finally, there is a burgeoning bulk of literature including White et al. (2019), Burniske and White (2017), and Symitsi and Chalvatzis (2019), that suggests Bitcoin should be classified as an entirely new asset class or type of technology altogether. PwC (2018) and Uhl et al. (2018) both consider Bitcoin a new type of intangible asset. Within this subdivision, ideas about regulatory bodies or frameworks are less apparent or nonexistent.

Purpose of this study

In the current environment, there seems to be a bureaucratic turf war between FinCEN, the CFTC, the SEC, and the IRS over the proper classification of Bitcoin and appropriate regulatory measures. This paper seeks to answer, what is the best way to classify and regulate Bitcoin to prevent money laundering and terrorist financing in the U.S.? It adds to the existing group of arguments that Bitcoin should be classified as a new type of technological asset, but it fills the gap in the literature by going beyond the existing legal regulatory frameworks to propose an entirely new framework for Bitcoin regulation.

This framework will be assessed according to how well it considers two criteria: the unique properties of Bitcoin and anti-money laundering/combating the financing of terrorism

(AML/CFT) concerns. Because Bitcoin was created specifically to avoid formal regulation, it is important that the framework addresses its unique properties – namely the P2P nature, decentralized organization, price volatility, and pseudo-anonymity – in order to effectively regulate it. Moreover, because of its potential to threaten national security by facilitating terrorist financing and money laundering, it is also important that these frameworks include appropriate AML/CFT measures for Bitcoin users.

CHAPTER 3: METHODS

This study will compare the existing legal frameworks – the BSA, the CEA, the Securities Act of 1933, the SEA, and the IRS’ 2014 Guidance – against my own framework for Bitcoin regulation. The effectiveness of these frameworks will be evaluated according to two criteria: how well they account for the unique properties of Bitcoin and how well they address AML/CFT concerns.

CHAPTER 4: DATA

This section will discuss the existing legal frameworks that have claimed jurisdiction over Bitcoin transactions. In each subsection, I will begin by giving a brief overview of the law. I will then analyze each framework according to how well it accounts for the unique properties of Bitcoin and how well it addresses concerns regarding money laundering and terrorist financing. I will then conclude by introducing and analyzing my own framework in the last subsection.

FinCEN: the BSA

Overview

The BSA was designed to detect and prevent money laundering and other criminal financial activities by requiring financial institutions to keep records and file reports “involving currency transactions and... customer relationships” (Federal Deposit Insurance Corporation 2005, 1). Such ‘financial institutions’ are defined as “[e]ach agent, agency branch, or office within the [U.S.] of any person doing business, whether or not on a regular basis or as an organized business concern” (U.S. Government Publishing Office 2020). This includes entities such as U.S. banks, savings associations, insurance companies, casinos, and, importantly, MSBs (Office of the Comptroller of the Currency n.d.; OFAC Sanctions Attorney, n.d.).

An MSB is defined as “[a] person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States” and includes entities that issue, sell, or redeem money orders or traveler’s checks; exchange foreign currencies; act as money transmitters; cash checks; and provide or sell Prepaid Access (Financial Crimes Enforcement Network n.d.). Crucially, an MSB does not include “[a] person registered with, and functionally regulated or examined by, the SEC or the CFTC” (U.S. Government Publishing Office 2020).

Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) are the two main means through which financial institutions are required to disclose their transactions under the BSA (Federal Deposit Insurance Corporation 2005, 1). A financial institution must complete a CTR for transactions over \$10,000 and is required to include certain personally identifiable information (PII) about the person conducting the transaction, including: their name, street address, social security number (SSN) or taxpayer identification number (TIN) if they are a non-U.S. resident, and their date of birth (2). A financial institution is required to submit a SAR for “any transactions aggregating \$5,000 or more that involve potential money laundering, suspected terrorist financing activities, or violations of the BSA” (45). The SAR form includes PII such as: the name of the customer and any other suspects, SSN or TIN, and the customer’s account number (45).

In 2019 FinCEN issued a Guidance claiming that any entities dealing in convertible virtual currencies (CVC), which includes Bitcoin, were considered MSBs under the ‘money transmitter’ provision (Financial Crimes Enforcement Network 2019a, 1). FinCEN argued:

“...as money transmission involves the acceptance and transmission of value that substitutes for currency by any means, transactions denominated in CVC will be subject to FinCEN regulations regardless of whether the CVC is represented by a physical or digital token, whether the type of ledger used to record the transactions is centralized or distributed, or the type of technology utilized for the transmission of value” (7).

In this way, entities that accept and transmit Bitcoin are required to register as an MSB under the BSA, and they are therefore subject to BSA reporting requirements, which include filing CTRs and SARs.

Bitcoin properties covered

Within this framework, Bitcoin is considered to be a currency. This is problematic for several reasons. First, “Bitcoin is not issued nor sanctioned by the US, or by any government” and therefore cannot be considered legal tender (Mandjee 2015, 167). In other words, it cannot

be accepted “for all debts, public charges, taxes, and dues” and therefore does not operate like traditional fiat currencies (U.S. Department of the Treasury 2011). Second, the production of bitcoins is capped at 21 million, after which no more bitcoins will be ‘minted’, or mined. This arguably undermines its effective use as a currency, as it is restricted in use unlike fiat currencies, which can be widely and infinitely used and exchanged.

Third, Bitcoin categorically does not fit the three main functions of money: a medium of exchange, a unit of account, and a store of value. As a medium of exchange, Bitcoin must be recognized by others as an acceptable mechanism for which people can exchange goods, services, or assets (Cohn 2016, 139). This is partially true for Bitcoin; in some cases, Bitcoin “is actually used to exchange goods and services, to allow a trade without direct use of goods” (Mandjee 2015, 169).

However in reality, Bitcoin usage as a medium of exchange remains “miniscule” (Yermack 2015, 32). Indeed several countries have outright banned the use of Bitcoin altogether, including Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan, the United Arab Emirates, and Vietnam (Library of Congress 2018, 4). This excludes a plethora of countries – among them China, Saudi Arabia, Iran and Colombia – where there is an “implicit ban” on Bitcoin usage (4). These bans have most likely contributed to the fact that only a handful of major retail companies accept payment in Bitcoin, which is indicative of the fact that it is not an appropriate or effective medium of exchange. Moreover, a user must actually possess bitcoins in order to transact with them, whereas people can conveniently make purchases without cash through the use of a credit card (Yermack 2015, 37).

As a unit of account, Bitcoin must “[place] a value or price on goods, services, or assets” (Cohn 2016, 139). This is undermined significantly by the extreme degree to which the price of

Bitcoin fluctuates. Figure 3 illustrates this volatility by showing that Bitcoin fluctuates much more on a daily basis than other fiat currencies and commodities (Gulker 2019).

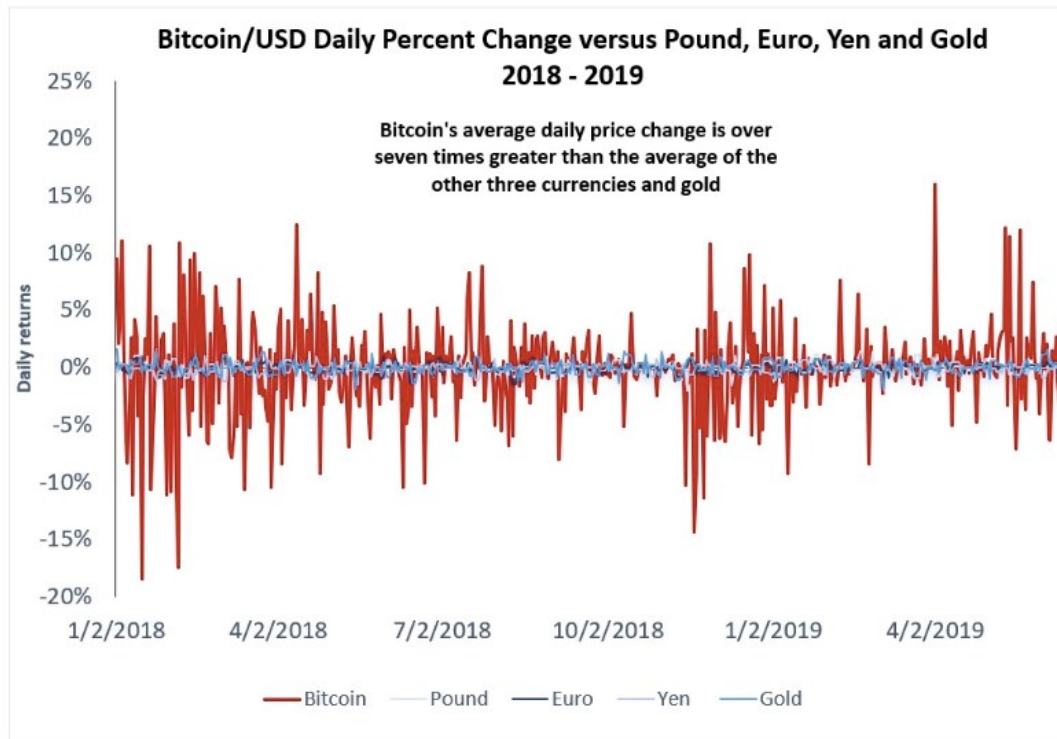


Figure 3: Comparison of Daily Fluctuations in the Price of Bitcoin

Because Bitcoin's price fluctuates so quickly and so dramatically, it is difficult for vendors to "establish a valid reference point for setting consumer prices" (Yermack 2015, 38). Consequently, many vendors must rely on "unwieldy price aggregates", such as the average price of bitcoins in exchanges over the last 24 hours, which results in different markets selling bitcoins for (sometimes significantly) different values at any given time (38). Such aggregations are logically not representative of the actual price of bitcoins in real time (38). This is highly problematic, as vendors could perhaps sell a bitcoin for much less or much more than what it is truly worth. From this discussion, it is clear that Bitcoin's volatility precludes it from accurately and continually serving as an effective unit of account. Rather, considering its unpredictability, Bitcoin may be better reflective of a speculative asset and potentially facilitate or otherwise

encourage arbitrage, which undermines the final function of money (Nian and Chuen 2015, 11; Yermack 2015, 38; Hougan, Kim, and Lerner 2019, 2).

Finally, as a “store of value”, Bitcoin must work to “preserve purchasing power or wealth in the private sector for investment purposes, or by governments in official foreign exchange reserves” (Cohn 2016, 139). While once procured, bitcoins technically do not have to be spent immediately and therefore can maintain value, the significant fluctuation of their value undermines their ability to “[retain their] purchasing power over time with a good deal of certainty” (Butler and Boylan 2010).

FinCEN argues that Bitcoin can be considered “a medium of exchange that can operate like currency but does not have all the attributes of ‘real’ currency... including legal tender status” (Financial Crimes Enforcement Network 2019a, 7). I find this conceptualization fundamentally contradictory to the true meaning of a currency, as the U.S. Department of Treasury, under which FinCEN is located, argues that in order to be seen as “a valid and legal offer of payment for debts when tendered to a creditor”, currency must have legal tender status (U.S. Department of the Treasury 2011). Considering this contradiction, and the above discussion regarding Bitcoin’s unsuitability as currency, it is clear that the regulatory framework proposed by FinCEN does not effectively account for the unique properties of Bitcoin.

AML/CFT protections covered

As the foremost AML law in the U.S., the BSA logically addresses many AML/CFT concerns. The extensive reporting requirements, namely registering with FinCEN as an MSB and submitting CTRs and SARs, has significantly contributed to cracking down on money laundering, terrorist financing, and other criminal financial activities in the U.S.

In one noteworthy case, officials prosecuted seven individuals involved in an online bitcoin exchange “on charges of operating unlicensed money transmitting businesses, as well as fraud, conspiracy, and bribery” (Financial Crimes Enforcement Network 2019b). Despite such successes, there are some noteworthy loopholes in the BSA that criminals can exploit using Bitcoin.

First, using Bitcoin “to purchase real or virtual goods or services will not transform a user into an MSB”, and therefore this user will not be subject to the same regulatory requirements as an MSB (Bryans 2014, 458). This is problematic, as it does not account for instances where an individual uses Bitcoin to purchase arms or any other critical materials that can then be sold or donated to terrorist groups. Indeed it does not even apply to Bitcoin donations to terrorist groups in general; it would only matter if the terrorist group bought the bitcoins.

Second, criminals can circumvent the \$10,000 and \$30,000 reporting thresholds for CTRs and SARs respectively, by transacting in smaller denominations of Bitcoin (Bryans 2014, 456). Finally, according to FinCEN, an entity that is already regulated by the SEC or the CFTC cannot be considered an MSB and therefore is not subject to regulations under the BSA. As U.S. regulatory bodies grapple with determining appropriate regulatory responsibility, criminals can benefit from this confusion by using Bitcoin in specific ways such that they would be under the jurisdiction of certain bodies whose regulations would have lesser repercussions or oversight regarding money laundering and terrorist financing activities.

The CFTC: the CEA

Overview

The CEA was created to regulate the trade of commodities futures (or the buying and selling of a commodity at a future date), in the U.S. so as to “foster open, transparent,

competitive and financially sound derivative trading markets and to prohibit fraud, manipulation and abusive practices in connection with derivatives and other products subject to the CEA” (U.S. Commodity Futures Trading Commission 2018, 1). As such, the CEA monitors illegal activities such as insider trading, market manipulation, and spoofing (Obie et al. 2019, 4-5).

The CEA recognizes four important groups: commodity pool operators (CPOs), commodity trading advisors (CTAs), futures commission merchants (FCMs), and introducing brokers (IBs). Put simply, a CPO “solicits, accepts, or receives from others, funds, securities, or property... for the purpose of trading in commodity interests” (Office of the Federal Registrar 2019, 67343). As the name suggests, a CTA is someone that advises others “as to the value of or the advisability of trading in commodity interests” (67343). An FCM “is an entity that solicits or accepts orders to buy or sell futures contracts, options on futures, retail off-exchange forex [foreign exchange market] contracts or swaps, and accepts money or other assets from customers to support such orders” (National Futures Association n.d.a). An IB essentially operates in the same way as an FCM, however IBs do not accept any money or other assets in support for these services (National Futures Association n.d.b).

Under the CEA, CPOs, CTAs, FCMs, and IBs are required to register with the CFTC and become members of the National Futures Association (National Futures Association n.d.c). By doing so, these firms are subjected to extensive reporting and compliance requirements, which include collecting PII and other sensitive information such as a customer’s name, address, occupation or business, previous experience with investments and futures trading, annual income, net worth, and age or date of birth (National Futures Association 2020, 5).

While the definition of a commodity under the CEA is very broad and has traditionally concerned products such as “agricultural commodities, metals, and energy”, the CFTC

determined in 2014 that Bitcoin satisfied the CEA’s definition (U.S. Commodity Futures Trading Commission 2014; U.S. Commodity Futures Trading Commission 2018, 1). As such, the CEA has jurisdiction “when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce” (U.S. Commodity Futures Trading Commission n.d.).

Bitcoin properties covered

Within this framework, Bitcoin is considered a type of commodity. At the surface level, it would appear that there is some merit to this argument. Indeed, Bitcoin has many similar attributes to other commodities, such as gold (Mandjee 2015, 178). For example, both are not regulated by a federal government, both have a finite supply, and both of their prices fluctuate much more when compared to fiat currencies (178-179). Moreover, it appears Bitcoin can be used like other commodities. As such, it can be effectively traded for other goods and services or currencies; it can be possessed, “as a specific user has control over distribution of its Bitcoin in his wallet”; and lastly, it is tangible to the extent that users “have ‘an appreciable ability to guide the destiny of Bitcoin’” (Mandjee 2015, 179; Johnson III 2012).

However, market analysis also demonstrates that Bitcoin does not consistently operate like other commodities. For example, a key attribute of gold is acting as “hedge and safe haven against assets such as stocks, bonds, and [the] US Dollar” (Klein, Thu, and Walther 2018, 106). Hedges and safe havens are financial instruments that enable investors to mitigate some financial risk during times of market turbulence. Thus, if Bitcoin is a true commodity akin to gold, it should act as a hedge or safe haven by enabling investors to maintain or even gain value during times of market distress.

While this has been true in some instances, Bitcoin performing as a hedge or safe haven remains inconsistent and highly contextual, confined to circumstances relating to certain geopolitical developments. For example, in mid-2019 at the height of the U.S.-China trade war, there was an acute rise in “demand for Bitcoin, especially among Chinese investors fearing a devaluing of the Yuan” (de Hallivand 2020). Similarly, in January 2020 after a U.S. airstrike killed Qassem Soleimani, the head of Iran’s Quds Force, “Bitcoin soared from under \$7,000 to almost \$8,500 for the week”, as investors anticipated “a prolonged escalation of tensions” (de Hallivand 2020). Figure 4 illustrates the correlations between Bitcoin’s rise in value alongside new developments in the ‘conflict’ (Martinez 2020).



Figure 4: Fluctuations in Bitcoin Amidst the 2020 U.S.-Iran Conflict

Interestingly, at the time of writing, Bitcoin has not acted in the same way in the wake of the global outbreak of novel coronavirus. Instead, in order to mitigate risk, investors are selling their riskiest assets. Coincidentally, these primarily appear to be Bitcoin holdings (Young 2020). As a result, on March 12, 2020, the price of Bitcoin plummeted from approximately \$8,000 to \$5,000, comprising “a loss of about 40% in the span of less than two days” (Shevchenko 2020).

Meanwhile, other traditional commodities such as gold and U.S. treasuries proved to be more resilient (Wilson and Carvalho 2020). Figure 5 depicts this relationship (Wilson and Carvalho 2020).



Figure 5: Yearly Performance Comparison of Bitcoin and Other Safe Haven Assets Amidst the Outbreak of Novel Coronavirus.

Taking this into consideration, it would seem that Bitcoin remains too small, too volatile, “less liquid, and costlier to transact (in terms of time and fees) than other assets... even in normal market conditions” (Young 2020; Smales 2019, 385). Therefore I argue that Bitcoin does not seem to fit completely under the classification of a commodity.

Even if the definition of a commodity were to be altered to address Bitcoin more specifically, the framework put forth by the CEA is problematic, as it is possible that many Bitcoin transactions would be exempt from the CEA under 17 C.F.R § 1.3. This clause clarifies that the term ‘future delivery’ “does not include any sale of a cash commodity for deferred

shipment or delivery”, which discounts the majority of Bitcoin transactions (Commodity Futures Trading Commission Act of 1974; Mandjee 2015, 180). In other words, the CFTC does not have jurisdiction over transactions where Bitcoin is exchanged for cash (Massad 2019, 32).

AML/CFT protections covered

CPOs, CTAs, FCMs and IBs are all considered ‘financial institutions’ under the BSA and therefore subject to AML/CFT reporting regulations (National Futures Association 2020, 6). In addition, FCMs and IBs are also responsible for submitting a “written customer identification program” (CIP) to demonstrate that they are aware of their customers’ true identities. CIPs necessitate the disclosure of certain PII of customers such as: name, date of birth, residential or business address, and SSN or TIN (7). For non-U.S. citizens, FCMs and IBs must obtain a copy of some form of government identification, such as a passport, that contains a picture and provides evidence of nationality, as well as “a government issued identification number” (7-8).

FCMs and IBs are also required to submit SARs with FinCEN if certain transactions appear suspicious or “involve an aggregate of at least \$5,000 in funds or other assets” (National Futures Association 2020, 9). In addition, FCMs and IBs are prohibited from facilitating certain transactions with individuals or entities located in a country under a sanction regime delegated by the Office of Foreign Assets Control (OFAC) (13). Moreover, and they are “required to block funds from individuals or entities identified on OFAC’s list of Specially Designated National and Blocked Persons (13).

Despite this, there are still many loopholes in the CEA and CFTC regulation that criminals can exploit. First, criminals can ostensibly apply the same loopholes used to evade BSA regulations to also avoid detection by the CFTC. Second, because the CFTC does not have jurisdiction over Bitcoin exchanges for cash, criminals could potentially manipulate prices in

forward and options contracts, swaps, forex swaps, and Ponzi schemes. Criminals could funnel this surplus of cash into larger money laundering schemes or directly to terrorist groups. Even if the CFTC were to expand its jurisdiction “to the cash market of crypto-assets which are commodities”, it would obfuscate regulatory efforts by splitting jurisdiction between the CFTC and the SEC, again creating confusion that criminals could potentially exploit (Massad 2019, 39).

The SEC: The Securities Act of 1933 and the SEA

Overview

The Securities Act of 1933 was created to ensure that investors received accurate and reliable information about the nature of securities for sale by cracking down on “deceit, misrepresentations, and other fraud in the sale of securities” (U.S. Securities and Exchange Commission 2013). The SEA created the SEC as the entity responsible for securities oversight, charging it with overseeing “registration, disclosure, and antifraud provisions” as well as monitoring security exchanges, brokerage firms, transfer agents, clearing agencies, and securities self regulatory organizations such as the New York Stock Exchange (Ly 2014, 597; U.S. Securities and Exchange Commission 2013).

Registration of securities with the SEC requires companies to provide information about their business (including properties and management), a description of the securities offered, and financial statements (U.S. Securities and Exchange Commission 2013). However, some security offerings may be exempt from registration. Among these, crucially, are “private offerings to a limited number of persons or institutions” (U.S. Securities and Exchange Commission 2013).

The SEC has taken an inconsistent approach to Bitcoin regulation. On one hand, the SEC supports the CFTC’s designation of Bitcoin as a commodity and argues that “[f]raud and

manipulation involving bitcoin traded in interstate commerce are appropriately within the purview of the CFTC” (Clayton 2017). On the other hand, the SEC acknowledges that “products linked to the value of underlying digital assets, including bitcoin and other cryptocurrencies, may be structured as securities products subject to registration under the Securities Act of 1933” (Clayton 2017).

Bitcoin properties covered

There arise several issues when classifying Bitcoin as a security and attempting to apply the regulatory frameworks under the Securities Act of 1933 and the SEA. First, the SEA defines a security broadly and includes in its definition stocks, bonds, notes, and investment contracts (Ly 2014, 597; Mandje 2015, 176). Taking into consideration the unique properties of Bitcoin, it would appear that Bitcoin does not directly fit into any of these categories, perhaps with the exception of investment contracts.

Bitcoin does not fit the definition of a stock, as “Bitcoins do not carry a right to a dividend declared by an issuer, a right to vote on an issuer’s affairs or conduct, or, in fact, any kind of right to participate in the economic success of a juridical entity” (Alberts and Fry 2015, 10). In addition, Bitcoin neither constitutes a note nor a bond, as “transactions for or in Bitcoins do not themselves result in any continuing obligation of one party to pay another” (13). Instead, there is a possibility that Bitcoin could be representative of an investment contract.

In the landmark Supreme Court case *SEC v. Shavers*, the Supreme Court rejected the defendant’s claim that “the Bitcoin investments that he sold were not ‘securities’” and ruled that they constituted investment contracts and therefore were indeed securities (Alberts and Fry 2015, 14). This has incorrectly led to the assumption that Bitcoins are securities and therefore subject to SEC regulations (14).

In another landmark Supreme Court case, *SEC v. Howey*, the Supreme Court determined that an investment contract requires four features: a person must invest money, the money must be invested into a common enterprise, a person must expect to profit from the investment, and these expected profits must be “generated solely from the efforts of the promoter or a third party” (Ly 2014, 598). The SEC itself issued a ‘framework’ for guidance in determining whether Bitcoin, ICOs of Bitcoin in particular, constitutes an investment contract.

ICOs are similar to crowdfunding campaigns; many companies and individuals have been using ICOs as a way “to raise capital for their businesses and projects” (Nolan et al. 2018, 2; Clayton 2017). As such, ICOs enable “investors to exchange currency such as U.S. dollars or cryptocurrencies in return for a digital asset labeled as a coin or token” (Clayton 2017). An ICO bears resemblance to a security or a security offering “when the promoters of these offerings emphasize the secondary market trading potential of these tokens” (Clayton 2017).

In conducting a ‘Howey Test’, the SEC found that the investment of money element is usually “satisfied in an offer and sale of” Bitcoin, as is the common enterprise feature (U.S. Securities and Exchange Commission 2019, 2). In regards to expectations of profit from third parties, the SEC did not provide a definitive answer and instead provided numerous circumstances for consideration. The SEC itself acknowledges that “the framework is not intended to be exhaustive nor to provide formal legal advice”, but rather serves to help determine whether an ICO constitutes an investment contract and is therefore subject to SEC regulation (Huillet 2019).

Upon a more thorough review, it would appear that Bitcoin does not reasonably fit into the definition of an investment contract. First, in transactions involving Bitcoin, an individual simply pays money to purchase bitcoins; he or she is not *investing* in Bitcoin itself (Ly 2014,

598). Second, Bitcoin does not reasonably fit the investment contract criteria because in most circumstances, people who purchase bitcoins “in anticipation of profits do not expect these profits to result from the action of the promoter”; instead, they are usually the result of market forces (Alberts and Fry 2015, 20-21). Third, and relatedly, the fact that the SEC cannot definitely determine that Bitcoin is an investment contract (but rather must examine ICOs on a case-by-case basis) is arguably indicative of the fact that the SEA framework is not a good fit.

AML/CFT protections covered

In October 2019, the SEC, the CFTC and FinCEN issued a joint statement stressing that all companies “with registered digital assets” are subject to AML regulations under the BSA. Previously, “[t]rading and investing in digital assets [had] fallen into a regulatory gray area as to which existing laws apply” (Johnson 2019). However, the agencies clarified that regulations applied irrespective of whether broker-dealers were handling securities or commodities (Johnson 2019). Although the SEC has taken more comprehensive steps to address AML/CFT concerns, under this guidance, criminals can still exploit the same loopholes in the BSA.

Additional concerns arise from the fact that under the SEA, private and limited offerings need not be registered with the SEC. In this way, it is possible for terrorist groups or organized crime syndicates to offer private securities to a limited amount of individuals, for example certain previous donors, in order to raise or launder funds. Moreover, there are a number of concerns with ICOs in particular. First, an ICO can circumvent the SEC’s crowdfunding regulation if the issuer is located outside the U.S. and if it is “offered and sold through funding portals and broker-dealers that are registered under the [SEC]” (Nolan et al. 2018, 3).

Second, unlike an IPO where investors buy shares of a company, the tokens acquired in an ICO do not signify ownership in a company (Vorobyev 2018, 210). Moreover, an IPO

requires a prospectus case, whereas an ICO requires a “white paper” to outline important “information about the project, coins being offered, the rights available to investors, lifecycle of the project, other legal terms and conditions, and more” (Tiwari, Gepp, and Kumar 2019, 8). However, white papers tend to be significantly less detailed than a prospectus and do not “adhere to any specified guidelines” (8). This has presented to criminals “the possibility of raising real money without offering anything meaningful in exchange and without preparing any complex documentations” (Katarzyna 2019, 6). With this money, it is possible to engage in money laundering or terrorist financing.

The IRS: 2014 Guidance

Overview

In 2014, the IRS issued a Guidance stipulating that Bitcoin is considered a property for federal tax purposes (Internal Revenue Service 2014). As such, the market value, as well as the basis, of Bitcoin is determined by converting Bitcoin into U.S. dollars at the exchange rate listed on an exchange (Internal Revenue Service 2014). Individuals must include payments in Bitcoins when determining gross income. This is calculated by determining the market value in U.S. dollars of the Bitcoin payment on the day that the payment was received. Gross income also applies to the mining of Bitcoins (Internal Revenue Service 2014).

It is possible for an individual to have a taxable gain “[i]f the fair market value of property received in exchange for virtual currency exceeds the taxpayer’s adjusted basis of the virtual currency” (Internal Revenue Service 2014). The converse is true for a loss, however “[t]he character of the gain or loss generally depends on whether the virtual currency is a capital asset in the hands of the taxpayer” (Internal Revenue Service 2014). In other words, a capital gain or loss applies when the property is a capital asset such as a stock, bond, or another type of

investment property. An ordinary gain or loss applies to property that is not a capital asset, which includes “inventory and other property held mainly for sale to customers in a trade or business” (Internal Revenue Service 2014).

Bitcoin properties covered

Under this framework, Bitcoin is considered a type of property. This is problematic for several reasons. First, it would seem the properties of the Bitcoin system clash significantly with property law. For example, property law ensures there is an agreement between the sender and the recipient of a transfer (Lehmann 2019, 97). However, Bitcoin does not necessitate such an agreement. Instead, “[Bitcoin] merely relies on the fulfillment of technological requirements, namely the use of the correct private and public key” (97). Property law also assures that when a mistake has occurred, the transfer is voidable (103). However with Bitcoin, all transactions are irreversible so long as the necessary private key of the sender is matched with the correct corresponding public key of the recipient (104). In this way, Bitcoin “does not take into account mistakes, fraud, or improper threats” (105). These problems are exacerbated by the fact that it is extremely difficult to determine which national law has jurisdiction over a transaction. In property law, each transfer is subject to “a governing national law”, however Bitcoin’s international reach and pseudo-anonymous properties obfuscate the ability “to identify the state which has the closest connection” to the transfer (97).

Second, while Bitcoin can operate like a property, as discussed it can also function notably as a currency. More specifically, Bitcoin acts like a property in the sense that “holders often trade and barter with it”, however it also acts like a currency in so far that it can be used to purchase goods and services (Roman 2015, 454). The IRS’ Guidance “sent a panic through the industry” as users were primarily using Bitcoin as a payment mechanism and feared its

classification as property “signaled the death [of] Bitcoin’s chance at becoming a staple digital currency and even potential rival to conventional currency” (Lemchuk 2017, 346-347).

Finally, treating Bitcoin as a property means that it would no longer be fungible, which carries significant tax implications for everyday purchases. For example with fiat currencies, it does not matter whether a person uses a five dollar bill gifted from a friend or one “found on the ground” (Lemchuk 2017, 347). However with Bitcoin, “using a coin purchased at \$10 will have a different, less favorable tax consequence than using a coin purchased at \$50” (347).

AML/CFT protections covered

There are significant issues with placing jurisdiction over Bitcoin regulation with the IRS, especially in regards to preventing money laundering and terrorist financing. First, the IRS is concerned primarily with tax reporting and tax evasion, and therefore does not have mechanisms in place to directly address AML/CFT concerns. With this being said, however, the IRS has implemented reporting requirements to ensure “taxpayer compliance” (Mirjanich 2014, 228). As such, Bitcoin users must now “comply with the information reporting requirements applicable to other forms of property” such as Form 1099-B, which requires taxpayers to disclose transactions with third parties that surpass a certain dollar amount in miscellaneous income (228).

Second, under this framework, the onus is on the consumers to report taxable income resulting from their use of Bitcoin. This is problematic, as “the majority of people using the virtual currency for illicit transactions have not reported Bitcoin as part of their taxes” (Lovell 2019, 941). This is complicated by the fact that Bitcoin is pseudo-anonymous, which exacerbates the IRS’ ability to determine “what ‘gains’ or ‘losses’ are realized from the Bitcoins” (Roman 2015, 454-455).

Third, the extreme fluctuation in the price of Bitcoin obscures users' ability to determine its fair market value and basis (Lovell 2019, 942). This is exacerbated by the fact that users can purchase bitcoins from different vendors at different rates and at different times (Roman 2015, 455). This confusion has emboldened some criminals from underreporting or otherwise manipulating the amount in Bitcoin that they report to the IRS, enabling them to evade taxes and hide a portion of income that can be used for money laundering or terrorist financing (Lovell 2019, 942). Moreover, because Bitcoin is pseudo-anonymous, "it would be extremely difficult for the IRS to track down the records required to sufficiently audit the taxpayer" (Roman 2015, 455).

Finally, as a property, a user's bitcoins could be protected under the Fifth Amendment, which grants individuals rights to personal property. If so, this would make seizing a user's bitcoins extremely difficult, and it would require explicit and undeniable proof on the part of law enforcement agencies that the holder used the bitcoins for terrorist financing, money laundering, or other criminal activities. Logically, providing clear evidence is further complicated by the pseudo-anonymous property of Bitcoin.

My framework: Private Sector Self-Regulation

Overview

Bitcoin was created with the explicit purpose of operating outside the purview of formal, public sector, regulatory bodies. Thus, to create an effective regulatory framework, I argue responsibility should rest primarily with private sector technology companies. This is because despite all of the jurisdictional inconsistencies within the U.S. and across the globe, and no matter where a user is or when he or she is active, one factor remains the same: in order to

procure, access, transact in, or even store bitcoins, a user must have access to a technological device that is capable of connecting to the Internet.

As such, private sector technology companies should come together to create and maintain certain regulatory standards for the community of Bitcoin users. There already exists such a grouping: the W3C. This international conglomerate was founded in 1989 with the express purpose of creating “open standards to ensure the long-term growth of the Web” (World Wide Web Consortium n.d.). Members include various universities, commercial entities such as Amazon and Alibaba, technology companies like Microsoft and Toshiba, as well as a range of telecommunications companies such as AT&T, Huawei, Samsung, and Verizon. The W3C also involves several banks and payment systems, such as PayPal, Wells Fargo, Barclays Bank, and the Inter-American Development Bank. The W3C even contains a few governmental members, including the Scottish Government and the government offices of India and Hong Kong that deal with information technology.

Considering the wide range of actors involved and their different areas of expertise, I argue the W3C is in the best position to tackle effective Bitcoin regulation by imposing self-regulatory measures. It is in the W3C’s mission to promote safety of and trust in the Web, therefore it is in the W3C’s interest to ensure Bitcoin users are not abusing the system. The W3C has the added benefit of maintaining international membership. In this way, regulation can be centralized and standardized not just in the U.S., but also on an international level. This is crucial for two reasons: first, considering the transnational nature of terrorist financing and money laundering, this would greatly aid AML/CFT efforts in cases that span multiple international jurisdictions, by fostering greater communication and the pooling of resources. Second,

standardization would mitigate the legal and jurisdictional mosaic of international perspectives on Bitcoin use and regulation.

However, one major limitation to this framework is that there is no enforcement mechanism. In other words, private sector entities do not have the power to make arrests or issue fines. As such, regulation should be implemented in a three-tiered framework. This framework would adapt a strategy dubbed “real-world assisted virtual currency self-governance” (Guadamuz and Marsden 2015). In this way, the W3C would work with companies that provide services in Bitcoin – such as the purchase, sale, transfer, exchange, or storage of bitcoins – to create community standards and rules on best practices. State governments would bolster the W3C by acting as the legal muscle and providing certain enforcement mechanisms (Guadamuz and Marsden 2015).

To elaborate further, the first tier represents the Bitcoin users. They are subject to regulations enforced by Bitcoin companies. These Bitcoin companies assume the second tier position and are subject to regulation according to the standards agreed upon with the W3C in conjunction with state governments. The W3C is the main acting entity in the third tier, with oversight over the Bitcoin companies and users. However, the W3C would not be given this status without the permission of state governments. In addition, only state governments have the power to enforce legal action. In this way, state governments are considered part of the third tier, but they play more of a hands-off role as both a consultant and a policing force. In other words, state governments help the W3C establish and enforce standards for the community of Bitcoin users in accordance with Bitcoin companies, and state governments also take legal action whenever violations of these community standards occur. Figure 6 depicts this dynamic.

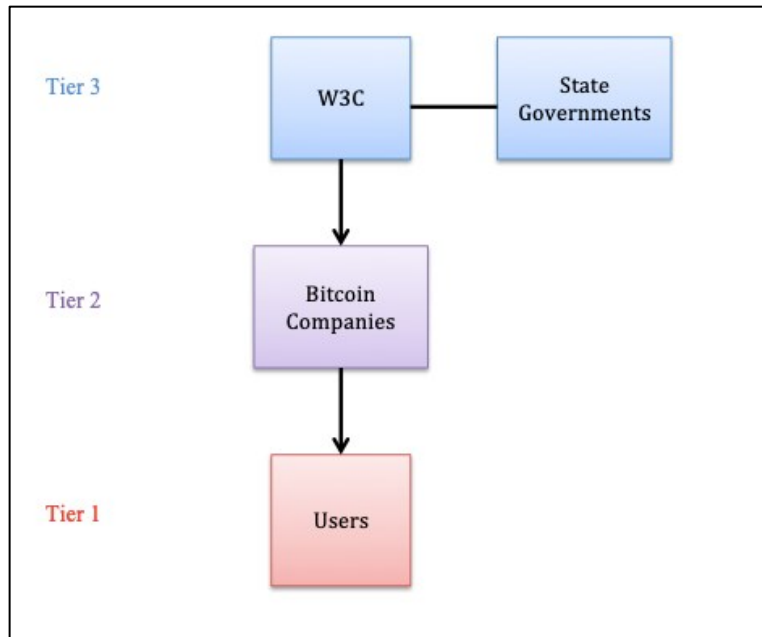


Figure 6: Flowchart for a Three-Tiered Framework for Bitcoin Regulation

Bitcoin companies enforce regulations through a contract that their customers and users must agree to upon registering and creating an account with the companies. These contracts would include certain terms and conditions that uphold W3C standards. Failure to comply with the terms and conditions would result in a user's account being suspended or terminated.

In a similar vein, Bitcoin companies must register with the W3C, and in this way, be subject to similar terms and conditions that they impose on their own users. Registering with the W3C enables Bitcoin companies to become accredited and legitimated on an international level. This would be a massive incentive for smaller, newer, and less-well known companies. It might also encourage countries that have banned the use of Bitcoin to reconsider, and thus registration would be an incentive for companies looking to expand their operations.

Finally, state governments allow this entire framework to operate. If at any point state governments do not agree to the standards, or if they feel the W3C is not effectively overseeing the regulatory measures, they can intervene and issue arrests or fines. Alternatively, they can

withdraw from the agreement and cease Bitcoin services within their borders. These punitive measures would incentivize the W3C to ensure regulation is up to par.

A potential ‘real-world’ parallel for this framework would be the Global Internet Forum to Counter Terrorism (GIFCT). The GIFCT was created in 2017 by Facebook, Microsoft, Twitter, and YouTube with the goal of promoting human rights and “[preventing] terrorists and violent extremists from exploiting digital platforms” (Global Internet Forum to Counter Terrorism n.d.a). The GIFCT’s membership is restricted exclusively to “companies operating internet platforms and services”, and besides the aforementioned four, also includes Pinterest, Dropbox, Amazon, LinkedIn, and WhatsApp (Global Internet Forum to Counter Terrorism n.d.c).

The GIFCT works closely with different companies, civil society groups, and government entities including the United Nations and the European Union in a “Multi-stakeholder forum” to define and identify terrorist activity (Global Internet Forum to Counter Terrorism n.d.a). There are three strategic pillars that underpin how the GIFCT and its stakeholders carry out its mission: prevent, respond, and learn (Global Internet Forum to Counter Terrorism n.d.a).

‘Preventing’ includes ensuring digital platforms and civil society groups are equipped with the proper “awareness, knowledge and tools, including technology, to develop sustainable programs in their core business operations to disrupt terrorist and violent extremist activity online” (Global Internet Forum to Counter Terrorism n.d.a). As part of this initiative, the GIFCT has created the Hash Sharing Consortium, which is committed to creating a database of hashes, or “unique digital ‘fingerprints’” of images or recruitment videos that have been associated with terrorist groups (Global Internet Forum to Counter Terrorism n.d.b). Sharing these hashes

enables other platform and service providers to remove content with the same hashes or preemptively block it before it is posted (Global Internet Forum to Counter Terrorism n.d.b).

‘Responding’ involves working with stakeholders to develop the tools necessary to mitigate the effects of a terrorist attack. This includes a Content Incident Protocol, which is designed to track terrorist events in real-time, such as live streams or posts from suspected terrorists, and alert the appropriate law enforcement officials (Global Internet Forum to Counter Terrorism n.d.b). Finally, ‘learning’ includes information sharing, support for research, and cooperation across private and public sector entities in order to improve “best practices for multi-stakeholder cooperation and [prevent] abuse of digital platforms” (Global Internet Forum to Counter Terrorism n.d.a).

In parallel to the Bitcoin framework, the W3C is similar to the GIFCT in the sense that they are both international bodies composed primarily of private-sector technology companies that establish guidelines and standards for a community. Both are responsible for regulating users of their platforms, and at the same time, both work with and answer to state governments on legal issues and strategies for implementation.

Bitcoin properties covered

Within this framework, Bitcoin is considered a type of technology. Although Bitcoin does bear certain hallmarks of a currency, a commodity, a security, and a property, the preceding paragraphs in this section have demonstrated that Bitcoin does not effectively fit into any of these categories. Instead in order to best regulate Bitcoin, it should be classified as a technology with financial components, and it should be included in the growing financial technology (FinTech) industry.

This is because the entire basis of Bitcoin functionality rests upon the Blockchain technology. While the Blockchain can be applied to other non-financial sectors, Bitcoin categorically would not be able to exist without the Blockchain. In other words, the Blockchain technology is so integrated into the Bitcoin system that Bitcoin should also be considered a new type of technology. What sets Bitcoin apart from other technologies, however, is its financial component: its ability to possess monetary value that can be traded for goods and services or exchanged for fiat currencies.

Bitcoin's technical and financial properties make it a good candidate to be included as a new technology in the burgeoning FinTech industry. 'FinTech', a combination of 'finance' and 'technology', is an "umbrella term" referring to "innovative financial solutions enabled by IT [information technology]" (Puschmann 2017, 70). In other words, FinTech encompasses technological innovations that impact the business and finance sector. Some examples of FinTech include "cryptocurrencies and the blockchain, new digital advisory and trading systems, artificial intelligence and machine learning, peer-to-peer lending, equity crowdfunding and mobile payment systems" (Philippon 2016, 2). From this discussion, it is clear that Bitcoin fits under the category of FinTech and should thus be regarded as a new technology with financial components and impacts.

AML/CFT protections covered

Under this framework, any companies offering services in Bitcoin including the purchase, sale, exchange, or storage of bitcoins in a wallet would be required to register with the W3C. Registration would give each company credibility, legitimacy, and access for its users on W3C members' technological devices. For example, registration would enable a Bitcoin exchange company to offer its app in the Apple App Store and run on Apple products. In return,

companies would be required to provide services in such a way so as to prevent users from facilitating terrorist financing or money laundering. Companies would also be subject to routine audits conducted by the W3C to examine records on users' activity.

There are a number of measures to ensure Bitcoin companies and users comply with community AML/CFT rules. First, Bitcoin companies could mandate users to disclose certain PII including a name, address, SSN, or TIN upon creation of an account. In the event that the company discovers potential illicit activity associated with a user, the company would be required to suspend that user's account and submit an activity report to the W3C. If there is explicit evidence that a user was using bitcoins for terrorist financing and money laundering, the company must immediately terminate that user's account, which may result in the loss of his or her bitcoins. The company would also be required to disclose the user's identity to the proper governmental authorities to take appropriate legal action. Failure to do so would result in these companies being blacklisted from offering their services on the technological devices developed by W3C members.

There is precedent that this strategy is effective. For example, in 2019 Apple contemplated removing Coinbase Wallet from the App Store for non-compliance issues (Haan 2019). This followed Google's temporary move to remove MetaMask, the Android equivalent of a bitcoin wallet, from Google Play (Haan 2019). Google determined that MetaMask was in violation of Google's rule to prohibit mining on mobile devices. This rule is most likely in place to prevent hackers from using "malware (infectious software) to commandeer vast 'bot-nets' (zombified networks of hacked devices belonging to innocent parties) for the surreptitious mining of cryptocurrencies" (Haan 2019). In both instances, the apps were allowed to remain

available through the respective stores after being reconfigured to fit Apple and Google’s compliance policies.

Second, the W3C could also enforce AML/CFT measures by maintaining a “redlist” of “the hashes [cryptographic algorithms] which identify wallets that have been involved in criminal activities” (Dinesh, Gilfoyle and Richard 2014, 4). This is similar to the GIFCT’s Hash Sharing Consortium. Once on the redlist, the W3C could prohibit Bitcoin companies from carrying out transactions connected with these wallets (4). This would prevent individuals from donating bitcoins to a redlisted wallet associated with a terrorist group, for example. Such a refusal “would make the value of the coins [already] in criminal wallets practically worthless, since no transactions can be conducted with them” (4). This would additionally prevent terrorists or other criminals from exchanging these coins for fiat currencies in furtherance of their illicit activities.

Finally, the W3C could implement AML/CFT protections by necessitating that companies offering certain services in Bitcoin – namely international remittances, charitable donations to religious or non-profit organizations, and exchanges for fiat currencies – complete and submit detailed reporting forms. These forms would include the reason for the transaction, the amount of the transaction, and PII such as the names of the sender and recipient of the bitcoins, their addresses, and their SSN, TIN, or other government-issued identification number. The reason these services are singled-out specifically is because these are some of the most popular ways terrorist groups have procured funding and criminals have disguised finances at the placement and layering stages of sophisticated money laundering schemes.

Before moving on, it is worth mentioning the benefits this framework has over the others that would be in the interest of all actors involved. First, each framework instructs users to

disclose sensitive PII in reporting requirements. This undermines Bitcoin’s attractive pseudo-anonymous quality. However in my framework, I argue that users will be more willing to reveal this information directly to private sector entities as opposed to state governments. Indeed, a 2017 survey conducted by PwC indicated that 72 percent of respondents thought “companies [were] better equipped than government to protect their data” (Spain et al. 2017, 3).

There are also several benefits to the framework that would be in the interest of all actors involved. First, as previously discussed, registering with the W3C gives Bitcoin companies legitimacy from which they obviously benefit. However, as more companies are incentivized to register, competition for fair pricing and services increases, which benefits users.

Second, as companies gain more legitimacy, countries that have banned the use of Bitcoin might be encouraged to reconsider. This would contribute to the growth of Bitcoin usage worldwide, which would benefit Bitcoin companies by increasing profits. It would also benefit users – especially “the unbanked and underbanked” – by introducing a new, acceptable payment system (Nian and Chuen 2015, 13). Moreover, this framework fosters greater public-private sector cooperation while ensuring checks and balances so that neither private sector nor public sector entities have a monopoly on the control of Bitcoin transactions.

Finally, there are several noteworthy benefits to self-regulation. For example, self-regulation can “be more cost-effective for governments, to the extent that enforcement and monitoring burdens are lightened and/or shifted to business” (Organisation for Economic Co-operation and Development 2015, 5). In addition, by eschewing government-imposed regulations, private sector self-regulation also promises to be “a more flexible instrument that could be adapted more easily to deal with changing conditions” (6). Relatedly, by maintaining self-regulation according to agreed-upon community standards, participants in the Bitcoin

system are more likely to abide by the regulations as opposed to measures imposed from above. This has further benefits, as it may mitigate the risk of over-regulation, which could result in the reduction of industry innovation, capital flight, and it could push users farther into the ‘dark corners’ of the Internet where regulations are more lax but where illicit activities such as terrorist financing and money laundering are more prevalent (Avan-Nomayo 2019). Table 1 summarizes the main points analyzed in this section.

Frameworks Criteria	FinCEN: BSA	CFTC: CEA	SEC: Securities Act of 1933 / SEA	IRS: Guidance	My framework: W3C
Bitcoin properties	<ul style="list-style-type: none"> Bitcoin is a currency Is not an effective medium of exchange, or a unit of account, or store of value Undetermined by 21 million cap and extreme price fluctuations Bitcoin is still not accepted at some major retailers 	<ul style="list-style-type: none"> Bitcoin is a commodity Not federally regulated, has a finite supply, can be traded Does not consistently act like a hedge or safe haven 	<ul style="list-style-type: none"> Bitcoin is a security Bitcoin does not fit the definition of securities such as stocks, bonds, notes and investment contracts An ICO is similar to an investment contract, but in most circumstances fails the Howey Test 	<ul style="list-style-type: none"> Bitcoin is a property Bitcoin properties complicate several factors of property law including making agreements on transfers and voiding fraudulent or mistaken transfers 	<ul style="list-style-type: none"> Bitcoin is a technology Technological and financial properties fit Bitcoin under FinTech industry
AML/CFT concerns	<ul style="list-style-type: none"> CTRs and SARs can deter criminals BSA applies to money transmitters, not users Criminals can evade reporting requirements by transacting in smaller amounts 	<ul style="list-style-type: none"> Subject to the BSA, the same loopholes apply CFTC does not have jurisdiction over Bitcoin exchanges for cash 	<ul style="list-style-type: none"> Subject to the BSA, the same loopholes apply Private and limited offerings do not need to register with the SEC 	<ul style="list-style-type: none"> Does not directly address AML/CFT concerns despite reporting requirements Price fluctuations may cause underreporting Relies on self-reporting, which can be abused by criminals 	<ul style="list-style-type: none"> Extensive reporting requirements, especially for remittances, donations, and fiat exchanges Redlisting wallets

Table 1: Evaluating Regulatory Frameworks

The x-axis lists the potential regulatory frameworks. The y-axis lists the evaluation criteria.

CHAPTER 5: DISCUSSION

In analyzing how Bitcoin fits into existing legal and regulatory frameworks in the U.S. – namely the BSA, the CEA, the Securities Act of 1933, the SEA, and the IRS’ 2014 Guidance – it is apparent that Bitcoin does not fit efficiently into any framework. Instead, I argue that Bitcoin should be classified as a new type of technology with financial components, and it should be grouped together with other technologies under the burgeoning FinTech industry. As such, regulation should rest with private sector entities, namely the W3C, in a three-tiered framework.

There are several significant limitations to this study. First, achieving international consensus on self-regulation led by the private sector will be extremely difficult. I anticipate it will take several years before certain countries such as Russia, China, and Iran opt-in to the framework. However, considering the benefits, these governments will likely come under pressure from businesses, individual users, and the international community, which may push these countries to consider adopting the framework.

Second, the focus of this paper is primarily on countering terrorist financing and money laundering. It is not necessarily concerned with tax evasion. Third, criminals can still evade this regulatory framework by transacting in Bitcoin on the Dark Web, where detection and prevention of terrorist financing and money laundering schemes is extremely difficult. In a similar vein, criminals may exploit jurisdictional inconsistencies between different countries. Fourth, and related, this framework does not necessarily apply to Bitcoin ATMs, with which a user does not need to create an account, register with a company, or use a traceable form of payment such as a credit card. In addition, users could evade detection by holding multiple wallets, or storing their bitcoins in a ‘hard’ wallet, which is essentially a flash drive.

Fifth, this research study represents a broad framework for regulating Bitcoin as a technology. It is intended to provide guidance and direction, but not specific details that will work in every context. As such, this study would benefit from more research to determine specific mechanisms besides redlisting to better detect and prevent terrorist financing, money laundering, and other illicit activities. This study would also benefit from further research to determine whether the three-tiered framework can be applied to other prominent cryptocurrencies and to examine how it would be impacted by the emergence of government-sponsored virtual currencies.

Finally, and most importantly, this framework could be rendered obsolete if the price of Bitcoin were to stabilize dramatically and consistently. Of the four existing legal frameworks analyzed in this paper, Bitcoin least problematically fits into the framework proposed by the CFTC. If the price of Bitcoin stabilizes, Bitcoin could reasonably be conceived of as a type of commodity, and it could be effectively regulated under the CEA. However, the price of Bitcoin is unlikely to stabilize in the near future to the same level of other commodities such as gold. Moreover, even if Bitcoin were subject to CEA regulations in the U.S., the same might not be said for other countries. In contrast, my framework benefits from international consensus that Bitcoin is a technology that should be regulated by private sector entities.

CHAPTER 6: CONCLUSION

Since Bitcoin was first created in 2008, it has introduced advantages equally as it has complications. On one hand, Bitcoin holds promise as a new, international payment system, serving those who live in regions where the formal banking sector is compromised by widespread corruption, or where it ceases to exist altogether. On the other hand, Bitcoin also poses an acute threat to national security, as terrorists and criminals have exploited Bitcoin's P2P and pseudo-anonymous nature in furtherance of their illicit activities. Consequently, there has been an international impetus in recent years to classify Bitcoin and determine an appropriate regulatory framework. As a result, there has developed an international mosaic of jurisdictional inconsistencies, with classification split mostly between a currency or an asset, and regulation ranging from an outright ban on Bitcoin usage to passive tolerance.

Within the U.S. itself, there has emerged a bureaucratic turf war between FinCEN, the CFTC, the SEC, and the IRS over how best to conceptualize and regulate Bitcoin. In examining the existing legal frameworks imposed by each entity – respectively: the BSA, the CEA, the Securities Act of 1933 and the SEA, and the IRS' 2014 Guidance – it is clear that none truly account for the unique properties of Bitcoin, nor do they effectively address AML/CFT concerns.

This paper goes beyond the existing legal frameworks in arguing that Bitcoin should be classified as a technology with financial components and regulated as a part of the growing FinTech industry. As such, regulation should rest primarily with private sector entities. The W3C, considering its membership and mission, is poised to assume such a role. Regulation will occur through a three-tiered framework according to shared community standards and rules for best practices. At the bottom in the first tier are individual users who are subject to regulation by

Bitcoin companies, which represent the second tier. These Bitcoin companies are, in turn, regulated by the W3C with support from state governments.

Safety and efficiency need not be zero-sum. Classifying Bitcoin as a technology and implementing an international, bottom-up, regulatory framework will enable the international community to more effectively counter terrorist financing and money laundering. In this way, Bitcoin can then serve its founding purpose: to integrate the underbanked and unbanked into the global financial system.

REFERENCES

- Alberts, Jeffrey E. and Bertrand Fry. 2015. "Is Bitcoin a Security?" *Boston University Journal of Science and Technology Law* 21, no. 1 (2015): 1-21.
https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jstl21&id=9&men_tab=srchresults#.
- Avan-Nomayo, Osato. 2019. "Pushing for Crypto Self-Regulation Amid Tightening Government Scrutiny." *Cointelegraph*, October 12, 2019. <https://cointelegraph.com/news/pushing-for-crypto-self-regulation-amid-tightening-government-scrutiny>.
- Baur, Dirk G., Kihoon Hong, and Adrian D. Lee. 2015. "Bitcoin: Medium of Exchange or Speculative Assets?" 1-31. <http://dx.doi.org/10.2139/ssrn.2561183>.
- Bollen, Rhys. 2013. "The Legal Status of Online Currencies: Are Bitcoins the Future?" *Journal of Banking and Finance Law and Practice* (May): 1-38.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285247.
- Brill, Allan and Lonnie Keene. 2014. "Cryptocurrencies: The Next Generation of Terrorist Financing?" *Defence Against Terrorism Review* 6, no. 1 (Spring and Fall): 7-30.
http://insct.syr.edu/wp-content/uploads/2015/05/Brill_Cryptocurrencies.pdf.
- Bryans, Danton. 2014. "Bitcoin and Money Laundering: Mining for an Effective Solution." *Indiana Law Journal* 89, no. 1 (Winter): 441-472.
<http://www.repository.law.indiana.edu/ilj/vol89/iss1/13>.
- Burniske, Chris and Adam White. 2017. *Bitcoin: Ringing The Bell For A New Asset Class*. New York, NY: Ark Invest Research. https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf.
- Butler, John and Jon Boylan. 2010. "Is Money a Store of Value?: The Amphora Report." *Financial Sense*, March 11, 2010. <https://www.financialsense.com/contributors/john-butler-john-boylan/is-money-a-store-of-value>.
- Carrick, Jon. 2016. "Bitcoin as a Complement to Emerging Market Currencies." *Emerging Markets Finance and Trade* 52, 10 (August): 2321-2334. DOI: 10.1080/1540496X.2016.1193002.
- Carroll, Paul and James Windle. 2018. "Cyber as an enabler of terrorism financing, now and in the future." *Journal of Policing, Intelligence and Counter Terrorism* 13, no. 3 (August): 285-300. DOI: 10.1080/18335330.2018.1506149.

- Carter, Shan and Amanda Cox. 2011. "One 9/11 Tally: \$3.3 Trillion." *The New York Times*, September 8, 2011. <https://archive.nytimes.com/www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?hp>.
- Chason, Eric D. 2019. "How Bitcoin Functions As Property Law." *Seton Hall Law Review* 49, no. 129-191. <https://scholarship.law.wm.edu/facpubs/1896>.
- Chu, Jeffrey, Saralees Nadarajah, and Stephen Chan. 2015. "Statistical Analysis of the Exchange Rate of Bitcoin." *PLoS One* 10, no. 7 (July): 1-27. DOI:10.1371/journal.pone.0133678.
- Chuen, David Lee Kuo, ed. 2015. *Handbook of Digital Currency : Bitcoin, Innovation, Financial Instruments, and Big Data*, edited by David Lee Kuo Chuen. London: Elsevier Inc. <https://ebookcentral.proquest.com/lib/jhu/reader.action?docID=2042366#>.
- Claeys, Grégory, Maria Demertzis, and Konstantinos Efstathiou. 2018. "Cryptocurrencies and monetary policy." *Policy Contribution* no. 10: 1-12. https://www.agefi.fr/sites/agefi.fr/files/fichiers/2018/08/cryptomonnaies_bruegel.pdf.
- Clayton, Jay. 2017. "Statement on Cryptocurrencies and Initial Coin Offerings." Public Statements. Last modified December 11, 2017. <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>.
- Cohn, Theodore E. 2016. *Global Political Economy*. New York: Taylor & Francis.
- Colville, Edward. 2014. "Bitcoin: 'real world' currency or speculative investment?" *Lexology*, January 23, 2014. <https://www.lexology.com/library/detail.aspx?g=4cc94226-367c-44d0-9ba5-94aed79b1b92>.
- Commodity Futures Trading Commission Act of 1974. 17 C.F.R. § 1.3 (1974).
- Corbet, Shaen, Brian Lucey, Andrew Urquhart, and Larisa Yarovaya. 2019. "Cryptocurrencies as a financial asset: A systematic analysis." *International Review of Financial Analysts* 62: 182-199. <https://doi.org/10.1016/j.irfa.2018.09.003>.
- Corcoran, Kieran. 2018. "Criminals in Europe are laundering \$5.5 billion of illegal cash through cryptocurrency, according to Europol." *Business Insider*, February 12, 2018. <https://www.businessinsider.com/europol-criminals-using-cryptocurrency-to-laundry-55-billion-2018-2>.
- de Hallivand, Paul. 2020. "Why Didn't Bitcoin React Like a Safe Haven Asset to Coronavirus Fears?" *Crypto Briefing*, February 26, 2020. <https://cryptobriefing.com/why-didnt-bitcoin-react-like-a-safe-haven-asset-to-coronavirus-fears/>.

- Dion-Schwarz, Cynthia, David, Manheim, and Patrick B. Johnston. 2019. *Terrorist use of cryptocurrencies: Technical and organizational barriers and future threats*. Santa Monica, CA: RAND.
https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf.
- Dorfman, Jeffrey. 2017. "Bitcoin Is An Asset, Not A Currency." *Forbes*, May 17, 2017.
<https://www.forbes.com/sites/jeffreydorfman/2017/05/17/bitcoin-is-an-asset-not-a-currency/#748e08a32e5b>.
- Fanusie, Yaya. 2019. " Hamas Military Wing Crowdfunding Bitcoin." *Forbes*, February 4, 2019.
<https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#513804874d7f>.
- Federal Deposit Insurance Corporation. 2005. *Bank Secrecy Act, Anti-Money Laundering, And Office Of Foreign Assets Control*. Washington, DC: Federal Deposit Insurance Corporation. <https://www.fdic.gov/regulations/safety/manual/section8-1.pdf>.
- Financial Crimes Enforcement Network. 2019a. *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*. Washington, DC: Financial Crimes Enforcement Network. <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.
- n.d. "Am I an MSB?" Accessed February 27, 2020. <https://www.fincen.gov/am-i-msb>.
- 2019b. "FinCEN Holds Fifth Annual Awards Program to Recognize Importance of Bank Secrecy Act Reporting by Financial Institutions." News Releases. Last modified May 19, 2019. <https://www.fincen.gov/news/news-releases/fincen-holds-fifth-annual-awards-program-recognize-importance-bank-secrecy-act>.
- Fox, David. 2019. "Cryptocurrencies in the Common Law of Property." In *Cryptocurrencies in Public and Private Law*, edited by David Fox and Sarah Green, 139-176. Oxford: Oxford University Press.
- Fox, David and Sarah Green, eds. 2019. *Cryptocurrencies in Public and Private Law*. Oxford: Oxford University Press.
- Freeman, Michael. 2011. "The sources of terrorist financing: Theory and typology." *Studies in Conflict & Terrorism* 34, no. 6 (May): 461–475. DOI: 10.1080/1057610X.2011.571193.
- Glaser, Florian, Kai Zimmermann, Martin Haferkorn, Moritz Weber, and Michael Siering. 2014. "Bitcoin - Asset Or Currency? Revealing Users' Hidden Intentions." Twenty Second European Conference on Information Systems.
<https://pdfs.semanticscholar.org/3c7d/998b88bf48c88cf693625d2852706e7cb8e4.pdf>.

- Global Internet Forum to Counter Terrorism. n.d.a. “Global Internet Forum to Counter Terrorism: Evolving an Institution.” Accessed April 27, 2020. <https://www.gifct.org/about/>.
- n.d.b. “Joint Tech Innovation.” Accessed April 27, 2020. <https://www.gifct.org/joint-tech-innovation/>.
- n.d.c. “Members.” Accessed April 27, 2020. <https://www.gifct.org/joint-tech-innovation/>.
- Goldman, Zachary K., Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. 2017. *Terrorist Use Of Virtual Currencies: Containing the Potential Threat*. Washington, DC: Center for a New American Security. <http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf>.
- Grinberg, Reuben. 2011. “Bitcoin: An Innovative Alternative Digital Currency.” *Hastings Science & Technology Law Journal* 4, no. 1: 159-208. <https://ssrn.com/abstract=1817857>.
- Gronwald, Marc. 2019. “Is Bitcoin a Commodity? On price jumps, demand shocks, and certainty of supply.” *Journal of International Money and Finance* 29 (October): 86-92. <https://doi.org/10.1016/j.jimonfin.2019.06.006>.
- Guadamuz, Andres and Chris Marsden. 2015. “Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies”. *First Monday* 20, no. 12 (December). <https://doi.org/10.5210/fm.v20i12.6198>.
- Gulker, Max. 2019. “Bitcoin Remains Vastly More Volatile Than Traditional Currencies.” *American Institute for Economic Research*, June 28, 2019. <https://www.aier.org/article/bitcoin-remains-vastly-more-volatile-traditional-currencies>. <https://www.treasury.gov/resource-center/faqs/Currency/Pages/legal-tender.aspx>.
- Haan, Cali. 2019. “Coinbase CEO: Apple Prohibiting “Decentralized Applications” at App Store.” *Crowdfund Insider*, December 30, 2019. <https://www.crowdfundinsider.com/2019/12/155781-coinbase-ceo-apple-prohibiting-decentralized-applications-at-app-store/>.
- Hougan, Matthew, Hong Kim, and Micah Lerner. 2019. *Economic and Non-Economic Trading In Bitcoin: Exploring the Real Spot Market For The World’s First Digital Commodity*. Washington, DC: U.S. Securities and Exchange Commission. <https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5532931-185248.pdf>.

- Huillet, Marie. 2019. "SEC Staff Publish Framework for Determining if Digital Assets Are Investment Contracts." *Coin Telegraph*, April 3, 2019. <https://cointelegraph.com/news/sec-staff-publish-framework-for-determining-if-digital-assets-are-investment-contracts>.
- Internal Revenue Service. 2014. "Internal Revenue Bulletin: 2014-16." IRB. Last modified April 14, 2014. https://www.irs.gov/irb/2014-16_IRB#NOT-2014-21.
- Johnson, Katanga. 2019. "Digital assets subject to money-laundering, disclosure laws: U.S. regulators." *Reuters*, October 11, 2019. <https://www.reuters.com/article/us-usa-sec-digitalassets-fraud/digital-assets-subject-to-money-laundering-disclosure-laws-u-s-regulators-idUSKBN1WQ2EC>.
- Johnson III, Thomas. 2012. "What U.S. Regulations Apply to Bitcoins as Commodities?" *Bitcoin Titan & Trading Titan*, 2012. Accessed February 29, 2020. <https://blog.bitcointitan.com/post/17789738826/what-us-regulations-apply-to-bitcoins-as#>.
- Kaplanov, Nikolei M. 2012. "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation." *Loyola Consumer Law Review* 25, no. 1 (November): 111-174. <https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1920&context=lclr>.
- Katarzyna, Ciupa. 2019. *Cryptocurrencies: Opportunities, Risks And Challenges For Anti-Corruption Compliance Systems*. Paris: Organisation for Economic Co-operation and Development. <http://www.oecd.org/corruption/integrity-forum/academic-papers/Ciupa-Katarzyna-cryptocurrencies.pdf>.
- Klein, Tony, Hien Pham Thu, and Thomas Walther. 2018. "Bitcoin is not the New Gold – A comparison of volatility, correlation, and portfolio performance." *International Review of Financial Analysis* 59: 105-116. <https://doi.org/10.1016/j.irfa.2018.07.010>.
- La Huis, Troy M. and Thomas E. McKeown. 2017. *Virtual currency and risks for terrorist financing*. Chicago, IL: Crowe Horwath. https://www.sifma.org/wp-content/uploads/2018/01/Crowe-Horwath_AML-2018_Marketing-PDF.pdf.
- Lehmann, Matthias. 2019. "Who Owns Bitcoin? Private Law Facing the Blockchain." *Minnesota Journal of Law, Science & Technology* 21, no. 1 (93-136). <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1474&context=mjlst>.
- Lemchuk, Stephanie A. 2017. "Virtual Whats?: Defining Virtual Currencies in the Face of Conflicting Regulatory Guidances." *Cardozo Public Law, Policy and Ethics Journal* 15, no. 2 (Spring): 319-350. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/cardplp15&div=15&id=&page=>.

- Library of Congress. 2018. *Regulation of Cryptocurrency Around the World*. Washington, DC: Library Of Congress. <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf>.
- Lovell, Allison M. 2019. "Avoiding Liability: Changing the Regulatory Structure of Cryptocurrencies to Better Ensure Legal Use." *Iowa Law Review* 104, no. 2 (January): 927-955. <http://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=134341296&site=ehost-live&scope=site>.
- Low, Kelvin F. K. and Ernie G. S. Teo. 2017. "Bitcoins and Other Cryptocurrencies As Property?" *Law, Innovation and Technology* 9, no. 2 (September): 1-39. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3039960.
- Lyandres, Evgeny, Berardino Palazzo, and Daniel Rabetti. 2019. "Do Tokens Behave like Securities? An Anatomy of Initial Coin Offerings." *SSRN* (May): 1-58. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3287583.
- Mandjee, Tara. 2015. "Bitcoin, its Legal Classification and its Regulatory Framework." *Journal of Business and Securities Law* 15, no. 2: 157-218. <https://digitalcommons.law.msu.edu/jbsl/vol15/iss2/4/>.
- Martinez, Ali. 2020. "Bitcoin Shows Signs as Safe-Haven Asset During Global Turmoil." *Crypto Briefing*, January 10, 2020. <https://cryptobriefing.com/bitcoin-safe-haven-asset-global-turmoil/>.
- Massad, Timothy G. 2019. *It's Time to Strengthen the Regulation of Crypto-Assets*. Washington, DC: Brookings. <https://www.brookings.edu/wp-content/uploads/2019/03/Timothy-Massad-Its-Time-to-Strengthen-the-Regulation-of-Crypto-Assets-2.pdf>.
- McCallum, Bennet T. 2015. "The Bitcoin Revolution." *Cato Journal* 35, no. 2 (Spring/Summer): 347-356. <https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/2015/5/cj-v35n2-11.pdf>.
- Mirjanich, Nicole. "Digital Money: Bitcoin's Financial and Tax Future Despite Regulatory Uncertainty." *DePaul Law Review* 64, no. 1 (Fall 2014): 213-248. <https://heinonline.org/HOL/P?h=hein.journals/deplr64&i=219>.
- Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." <https://bitcoin.org/bitcoin.pdf>.
- National Futures Association. n.d. "Futures Commission Merchant (FCM) Registration." Registration. Accessed February 29, 2020. <https://www.nfa.futures.org/registration-membership/who-has-to-register/fcm.html>.

- n.d. “Introducing Broker (IB) Registration.” Registration. Accessed February 29, 2020. <https://www.nfa.futures.org/registration-membership/who-has-to-register/ib.html>.
- 2020. *NFA Regulatory Requirements*. Chicago, IL: National Futures Association. <https://www.nfa.futures.org/members/member-resources/files/regulatory-requirements-guide.pdf>.
- n.d. “Registration and Membership.” Registration. Accessed February 29, 2020. <https://www.nfa.futures.org/registration-membership/index.html>.
- Nian, Lam Pak and David LEE Kuo Chuen. 2015. “Introduction to Bitcoin.” In *Handbook of Digital Currency : Bitcoin, Innovation, Financial Instruments, and Big Data*, edited by David Lee Kuo Chuen, 5-30. London: Elsevier Inc. <https://ebookcentral.proquest.com/lib/jhu/reader.action?docID=2042366#>.
- Nolan, Anthony R.G., Edward T. Dartley, Mary Burke Baker, John ReVeal, and Judith E. Rinearson. 2018. “Initial coin offerings: key US legal considerations for ICO investors and sponsors.” *Journal of Investment Compliance* 19, no. 1: 1-9. DOI 10.1108/JOIC-02-2018-0016.
- Obie, Stephen J., Jayant W. Tambe, Ryan J. Andreoli, Céalagh P. Fitzpatrick, and Eric A. Love. 2019. *Commodity Exchange Act: Key Decisions from 2018 and Enforcement Trends to Monitor in 2019*. New York, NY: Jones Day. <https://www.jonesday.com/en/insights/2019/01/commodity-exchange-act>.
- OFAC Sanctions Attorney. n.d. “Financial Institutions and Businesses Regulated by Bank Secrecy Act.” Accessed February 27, 2020. <https://ofaclawyer.net/financial-institutions-under-bank-secrecy-act/>.
- Office of the Comptroller of the Currency. n.d. “Bank Secrecy Act (BSA) & Related Regulations.” Accessed February 27, 2020. <https://www.occ.treas.gov/topics/supervision-and-examination/bsa/bsa-related-regulations/index-bsa-and-related-regulations.html#>.
- Office of the Federal Registrar. 2019. “Rules and Regulations.” *Federal Registrar* 84, no. 273 (December 2019): 67343-67355. <https://www.govinfo.gov/content/pkg/FR-2019-12-10/pdf/2019-26161.pdf>.
- Organisation for Economic Co-operation and Development. 2015. *Industry Self-Regulation: Role And Use In Supporting Consumer Interests*. Paris: Organisation for Economic Co-operation and Development. [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP\(2014\)4/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2014)4/FINAL&docLanguage=En).

- Prentis, Mitchell. 2015. "Digital Metal: Regulating Bitcoin as a Commodity." *Case Western Reserve Law Review* 66, no. 2 (Winter): 609-638.
<https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2654&context=caselrev>.
- Philippon, Thomas. 2016. *The FinTech Opportunity*. Washington, DC: National Bureau Of Economic Research. <https://www.nber.org/papers/w22476.pdf>.
- Puschmann, Thomas. 2017. "Fintech." *Business & Information Systems Engineering* 59: 96-76.
<https://doi.org/10.1007/s12599-017-0464-6>.
- PwC. 2018. "Cryptocurrencies: Time to consider plan B." PwC point of view. Last modified March 6, 2018. <https://www.pwc.com/us/en/cfodirect/publications/point-of-view/cryptocurrency-bitcoin-accounting.html>.
- Reynolds, Perri and Angela S. M. Irwin. 2017. "Tracking Digital Footprints: Anonymity Within the Bitcoin System." *Journal of Money Laundering Control* 20, no. 2 (May): 172-189. DOI: 10.1108/JMLC-07-2016-0027.
- Schilling, Linda M. and Harald Uhlig. 2019. "Currency Substitution under Transaction Costs." *AEA Papers and Proceedings*, 109 (May): 83-87. DOI: 10.1257/pandp.20191017.
- Shahzad, Syed Jawad Hussain, Elie Bouri, David Roubaud, Ladislav Kristoufek and Brian Lucey. 2019. "Is Bitcoin a better safe-haven investment than gold and commodities?" *International Review of Financial Analysis* 63 (May): 322-330.
<https://doi.org/10.1016/j.irfa.2019.01.002>.
- Shevchenko, Andrey. 2020. "Coronavirus Has Put Bitcoin's Safe Haven Narrative to the Test." *Cointelegraph*, April 24, 2020. <https://cointelegraph.com/news/coronavirus-has-put-bitcoins-safe-haven-narrative-to-the-test>.
- Spain, David, Sean Joyce, Jocelyn Aqua, Jay Cline, and Matthew Lieberman. 2017. *Consumer Intelligence Series: Protect.me*. PwC. <https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf>.
- Swartz, Nicole D. 2014. "Bursting the Bitcoin Bubble: The Case To Regulate Digital Currency as a Security or Commodity." *Tulane Journal of Technology and Intellectual Property* 17: 319-335.
<https://heinonline.org/HOL/Page?handle=hein.journals/tuljtip17&div=11&id=&page=&collection=journals>.
- Symitsi, Efthymia and Konstantinos J Chalvatzis. 2019. "The Economic Value of Bitcoin: A Portfolio Analysis of Currencies, Gold, Oil and Stocks." *Research in International Business and Finance*, 48: 97-110. <https://doi.org/10.1016/j.ribaf.2018.12.001>.

- Tiwari, Milind, Adrian Gepp, and Kuldeep Kumar. 2019. "The future of raising finance - a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams." *Crime, Law and Social Change* (November): 1-25. <https://doi.org/10.1007/s10611-019-09873-2>.
- Turpin, Jonathan B. 2014. "Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework." *Indiana Journal of Global Legal Studies* 21, no. 1 (Winter): 335-368. <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1557&context=ijgls>.
- Uhl, Robert, Amy Steele, Ivan O'Donnell, Doug Zercoe, and Peter Taylor. 2019. *Classification of Cryptocurrency Holdings*. New York, NY: Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/ASC/FRA/2018/us-aers-fra-classification-of-cryptocurrency-holdings.pdf>.
- U.S. Commodity Futures Trading Commission. 2017 *A CFTC Primer on Virtual Currencies*. Washington, DC: CFTC. https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/labcfrc_primercurrencies100417.pdf.
- n.d. *Bitcoin Basics*. Washington, DC: CFTC. https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/oceo_bitcoinbasics0218.pdf.
- 2018. *CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets*. Washington, DC: CFTC. https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf.
- 2014. "Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry." Public Statements & Remarks. Last modified December 10, 2014. <https://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6>.
- U.S. Department of Justice. 2020. "Long Island Woman Sentenced to 13 Years' Imprisonment for Providing Material Support to ISIS." News. Last modified March 13, 2020. <https://www.justice.gov/opa/pr/long-island-woman-sentenced-13-years-imprisonment-providing-material-support-isis>.
- U.S. Department of the Treasury. 2011. "Legal Tender Status." Resource Center. Last modified January 4, 2011. <https://www.treasury.gov/resource-center/faqs/Currency/Pages/legal-tender.aspx>.
- U.S. Government Publishing Office. 2020. "§1010.100 General definitions." Electronic Code of Federal Regulations. Last modified February 26, 2020. https://www.ecfr.gov/cgi-bin/text-idx?SID=f7495bb4cb9f4181f1505d475bb7fb22&mc=true&node=se31.3.1010_1100&rgn=div8.

- U.S. Securities and Exchange Commission. 2019. *Framework for “Investment Contract” Analysis for Digital Assets*. Washington, DC: SEC. <https://www.sec.gov/files/dlt-framework.pdf>.
- 2013. “The Laws That Govern the Securities Industry.” Investor Information. Last modified October 1, 2013. <https://www.sec.gov/answers/about-lawsshtml.html>.
- Volastro, Anthony. 2014. “CNBC Explains: How to mine bitcoins on your own.” *CNBC*, January 23, 2014. <https://www.cnb.com/2014/01/23/cnbc-explains-how-to-mine-bitcoins-on-your-own.html>.
- Vorobyev, A.V. 2018. “ICO as Economic Security Threat. Possible Risks Analysis. Experience of Foreign States” in *FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies*, KnE Social Sciences: 208-214. 10.18502/kss.v3i2.1544.
- Wiseman, Scott A. 2016. “Property or Currency? The Tax Dilemma Behind Bitcoin.” *Utah Law Review* 2016, no. 2: 417-440. <https://dc.law.utah.edu/cgi/viewcontent.cgi?article=1018&context=ulr>.
- Wilson, Tom and Ritvik Carvalho. 2020. “Speculative bet or inflation hedge? Bitcoin in the coronavirus crisis.” *Reuters*, April 21, 2020.
- World Wide Web Consortium. n.d. “About W3C.” Accessed March 16, 2020. <https://www.w3.org/>.
- Yang, Ruoke. 2013. “When is Bitcoin a Security Under U.S. Securities Law?” *Journal of Technology Law & Policy* 18, no. 2: 99-130. <https://heinonline.org/HOL/Page?handle=hein.journals/jt1p18&id=113&collection=journals&index=>.
- Yermack, David. 2015. “Is Bitcoin a Real Currency? An Economic Appraisal.” In *Handbook of Digital Currency : Bitcoin, Innovation, Financial Instruments, and Big Data*, edited by David Lee Kuo Chuen, 31-43. London: Elsevier Inc. <https://ebookcentral.proquest.com/lib/jhu/reader.action?docID=2042366#>.
- Young, Joseph. 2020. “Why is the Bitcoin price crashing in tandem with the Dow Jones?” *Cryptoslate*, February 24, 2020. <https://cryptoslate.com/why-is-the-bitcoin-price-crashing-in-tandem-with-the-dow-jones/>.

CURRICULUM VITAE

Emily received her undergraduate degree in 2018 from the University of St Andrews in Scotland, where she graduated with an MA (Hons) First Class in Arabic and International Relations. Her undergraduate thesis explored how terrorism has impacted the perception of the Arabic language and Arabic-speaking peoples in the Western world. After graduation, Emily will begin a career as an analyst for the federal government.