

*Citation for published version:*

Fletcher, E, Larkin, C & Corbet, S 2021, 'Countering money laundering and terrorist financing: A case for bitcoin regulation', *Research in International Business and Finance*, vol. 56, 101387.  
<https://doi.org/10.1016/j.ribaf.2021.101387>

*DOI:*

[10.1016/j.ribaf.2021.101387](https://doi.org/10.1016/j.ribaf.2021.101387)

*Publication date:*

2021

*Document Version*

Peer reviewed version

[Link to publication](#)

*Publisher Rights*

CC BY-NC-ND

**University of Bath**

**Alternative formats**

If you require this document in an alternative format, please contact:  
[openaccess@bath.ac.uk](mailto:openaccess@bath.ac.uk)

**General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

**Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# Countering money laundering and terrorist financing: A case for Bitcoin regulation

Emily Fletcher<sup>a</sup>, Charles Larkin<sup>a,b,c</sup>, Shaen Corbet<sup>d,e\*</sup>

<sup>a</sup>*Kreiger School of Arts Sciences, Johns Hopkins University, Baltimore, MD, USA*

<sup>b</sup>*Institute for Policy Research, University of Bath, UK*

<sup>c</sup>*Trinity Business School, Trinity College Dublin, Dublin 2, Ireland*

<sup>d</sup>*DCU Business School, Dublin City University, Dublin 9, Ireland*

<sup>e</sup>*School of Accounting, Finance and Economics, University of Waikato, New Zealand*

*\* Corresponding Author: shaen.corbet@dcu.ie*

---

## Abstract

Bitcoin was created in 2008 to serve as an alternative payment mechanism for both the under-banked and un-banked, or those in regions where the formal financial system suffers from broad corruption and efficient regulation. 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 US 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.

*Keywords:* Money laundering; Terrorist Financing; Cryptocurrency; Regulation.

---

## 1. Introduction

Money, and broad illicit financing 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 organisations’ altogether ([53]). 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 [67]. Since the September 11 terrorist attacks, however, law enforcement agencies have established several effective counter-terrorist finance methods for thwarting the movement of fiat currencies, or government-issued currencies, to terrorist groups. However, some argue the success of such counter-terrorist finance programs may encourage terrorist groups to look elsewhere to finance their activities, namely the growing cryptocurrency market ([47]). It is worth mentioning that while there are several hundred different types of cryptocurrencies, the focus of this paper will be primarily on Bitcoin. This paper is primarily concerned with the regulatory responses made by the United States government with reference to interactions with global regulations. 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. Despite these benefits, the widespread popularity of Bitcoin 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-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 organisations and organized crime syndicates to abuse the Bitcoin system for terrorist financing, money laundering, and other criminal activities [45, 38]. Consequently, several regulatory bodies in the United States (U.S.) have endeavoured 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 Securities and

Exchange Commission (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 Internal Revenue Service (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 monitoring and 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 avoid regulation altogether. To avoid these issues, 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). Therefore, we 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 which 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. In the following research, we set out a variety of cases through which we investigate the potential to regulate Bitcoin (and by extension, other cryptocurrencies) to mitigate the effects of money laundering and terrorist finance.

The remained of the paper is structured as follows: in Section 2 we describe the related previous literature and research that has focused on a number of similar financial products. In Section 3 we present broad consideration of the multiple legal frameworks that exist across multiple jurisdictions. Section 4 presents a broad discussion of the issues that exist and the potential areas through which progress can be made, while Section 5 concludes.

## **2. Previous Literature**

Since the creation of the Internet in the early 1980s, everyday objects and transactions have become increasingly digitised, 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: centralised or decentralised/distributed. Examples of the former include ‘loyalty points’ from retail companies or ‘air miles’; they are confined within the centralised structure of a particular entity ([89]). Decentralised 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 ([86]), Bitcoin has gained significant publicity as the world’s first decentralised cryptocurrency and the current leader of the cryptocurrency market ([44]). 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’ ([86]). 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 decentralised and distributed open-source software platform, meaning that not only can anyone access it, but each user is connected to each other in the network and can leave or enter the network at any time ([89]). 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’ ([89]; [12]). 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 ([12]).

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’ ([89]). 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. 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. 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 ([12]). Figure 1 below depicts how a bitcoin transaction works using the public and private keys ([86]).

**Insert Figure 1 about here**

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 ([89]). 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. 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 ([89]). 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.

**Insert Figure 2 about here**

It is important to note that this schema only applies to public list blockchain. Blockchain technology can be applied to other activities, such as the verification of transactions and contracts without the need for third-party intermediaries. This application allows for cost-efficient trust relationships to be formed. Blockchain’s smart contracts (otherwise known as its business rule feature) puts in place an automatic sequencing and requirements which ensures that P2P transactions can take place seamlessly. A simple example of an alternative use, is that blockchain can be used to create permanent, immutable identification records for persons and firms, a step already taken by the Estonian government. This has the potential to become a growth area for governments outside of the cryptocurrency application and to bring about a wider acceptance of this technology. Ultimately, the technology is robust, based upon international standards, open source and easily used by end-users, which makes it ideal for actors seeking cost-efficient trust relationships that do not involve the facilitation or oversight of third parties.

Like all forms of blockchain, Bitcoin operates independently of a central authority such as a central bank<sup>1</sup>. It 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 ([21]). 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. However, there remains a number of severe criminality concerns with regards to 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 ([89]). 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

---

<sup>1</sup>For a detailed overview on the development of research surrounding Bitcoin in recent times, please see [43, 44, 73, 83, 72]

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. Secondly, 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’ ([93]). Third, and related, Bitcoin is attractive due to the ‘global reach and speed’ of transactions. 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. It also reduces the time horizons law enforcement agencies have to detect and intercept suspicious payments ([13]). Fourth, Bitcoin is attractive for its relative ease and low cost of use ([13]). Using Bitcoin arguably requires very little technical skill, and the only materials needed are devices that can be connected to the Internet ([13]). In this way, transferring bitcoins is as easy as sending an email.

Finally, the fact that payments are irreversible may be attractive to terrorist groups ([13]). There is no additional verification needed to finalise a payment, which enables transactions to be processed more quickly. 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. 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 an asset.

Most of the early literature surrounding the classification of Bitcoin (for example [69]) argues it should be treated as a new type of digital or virtual currency, alternative to traditional government-backed fiat currencies. [102] notes that Bitcoin is essentially the digital equivalent of cash, while [81] 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. [63] 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. [105] criticised 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. [94] create a model that demonstrates Bitcoin can compete as a viable alternative to traditional fiat currencies in the current monetary system, whereas [17] 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 has declared in 2013 that Bitcoin exchangers and administrators would be classified as Money Services Businesses (MSBs) and therefore are subject to strict reporting and registration requirements. The most comprehensive treatments of Bitcoin and cryptocurrencies as "money" are to be found in terms of economic theory in [1] and legally in [52] and [56].

When considering Bitcoin as an asset, the literature within this category is much less straightforward and divided into many subsections according to different types of assets. [106] argue that Bitcoin should be conceptualised more as some sort of 'speculative asset', as users exploit the volatile price fluctuations with a view towards maximising profits. [7] conduct studies analysing the behaviour 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<sup>2</sup>. Others argue that Bitcoin should be treated like a commodity. [64] compared the Bitcoin market to those of crude oil and gold to demonstrate that Bitcoin functions most like a commodity, whereas [95] discuss the viability of bitcoin as a safe haven asset in comparison to other commodities like gold. [80] 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. [98] 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 conceptualised as an investment contract. [39] state 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. It has been previously considered that if deemed a security, the main regulatory 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 it 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. [78] support this claim, citing private law rights. [19] argues that Bitcoin transactions resemble real estate property transactions. The IRS in the US determined in 2014 that Bitcoin should be considered a property for tax purposes, considering the repercussions for users arising from this framework of regulation. Finally, [100], that suggests Bitcoin should be classified as an entirely new asset class or type of technology altogether. Bitcoin is broadly considered to be a new type

---

<sup>2</sup>Detailed contributions with regards to the price behaviour and discovery of both Bitcoin and a number of broader cryptocurrencies have also been provided by [10, 11, 15, 107, 16, 88, 48, 79, 68, 97, 8, 50, 85, 20] and [74]



of intangible asset. Within this subdivision, ideas about regulatory bodies or frameworks are less apparent or nonexistent.

We first need to establish the 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, decentralised organisation, 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.

### 3. Consideration of the Legal Frameworks

This study will compare the existing US legal frameworks – the BSA, the CEA, the Securities Act of 1933, the Securities Exchange Act of 1934, and the IRS’ 2014 Guidance – against the discussed 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. This particular section will discuss the existing legal frameworks that have claimed jurisdiction over Bitcoin transactions. In each subsection, we begin by giving a brief overview of the law, while then analysing 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. We then conclude by introducing and analysing an alternative framework which could guide the regulation of Bitcoin and similar cryptocurrency.

#### 3.1. *FinCEN: the BSA*

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<sup>3</sup>’. 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

---

<sup>3</sup>Federal Deposit Insurance Corporation. 2005. Bank Secrecy Act, Anti-Money Laundering, And Office Of Foreign Assets Control. Washington, DC: FDIC. Available [here](#)

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 traveller’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. 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. 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’. 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.

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 2019). 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 centralised or distributed, or the type of technology utilised for the transmission of value’. 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.

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 ([80]). 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 recognised by others as an acceptable mechanism for which people can exchange goods, services, or assets ([22]). 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’ ([80]).

However in reality, Bitcoin usage as a medium of exchange remains minuscule ([106]). 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,). This excludes a plethora of countries – among them China, Saudi Arabia, Iran and Colombia – where there is an ‘implicit ban’ on Bitcoin usage. 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 ([106]). As a unit of account, Bitcoin must ‘[place] a value or price on goods, services, or assets’ ([22]). This is undermined significantly by the extreme degree to which the price of Bitcoin fluctuates. 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’ ([106]). 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. Such aggregations are logically not representative of the actual price of bitcoins in real time. 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 ([89]; [106]).

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. 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. We find this conceptualisation 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. 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 true properties of Bitcoin.

When considering the 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 ([14]). 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 ([14]). 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.

### *3.2. The CFTC: the CEA*

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). As such, the CEA monitors illegal activities such as insider trading, market manipulation, and spoofing. The CEA recognises four important groups: commodity pool operators (CPOs), commodity trading advisers (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’. 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).

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). 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 ([80]). 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. 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’ ([80]).

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. 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. 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.

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 [42] and [41]; that a number of characteristics expected during a “flight to safety” were present during the period analysed. The volatility relationship between the main Chinese stock markets and Bitcoin evolved significantly during this period of enormous financial stress. Such dynamic correlations during periods of stress present further evidence to cautiously support the validity of the development of this new financial product within mainstream portfolio design through the diversification benefits provided<sup>4</sup>. Other examples of herding and interaction with cryptocurrencies during the period of exceptional stress due to COVID-19 have also been addressed<sup>5</sup> by ([24]; [28] and [40])

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 ([80]). In other words, the CFTC does not have jurisdiction over transactions where Bitcoin is exchanged for cash. 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. 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’. 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). 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). Moreover, and they are ‘required to block funds from individuals or entities identified on OFAC’s list of Specially Designated National and Blocked Persons.

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

---

<sup>4</sup>For detailed analyses of a broad range of inherent issues relating to cryptocurrency correlations, please see the works of [33, 34, 82, 66, 54, 55, 9, 5, 30, 18, 59, 27, 70] and [71]. For related research focusing on the diversification benefits of Bitcoin and broader cryptocurrencies, please see the works of [96, 99, 3, 25, 2] and [35]

<sup>5</sup>For detailed analyses of analyses relating to the behaviour of cryptocurrency during crises, please see the works of [36, 37, 26, 23, 104, 32, 49, 51, 6, 4, 87, 29] and [31], and with regards to consideration during times of crisis inclusive of major discontinuities in trading conditions such as the arrival of COVID-19 and ongoing volatility due to political uncertainty, please see [62, 60, 58, 57] and [61]

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.

### 3.3. The SEC: The Securities Act of 1933 and the SEA

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’. The SEA created the SEC as the entity responsible for securities oversight, charging it with overseeing ‘registration, disclosure, and anti-fraud provisions’ as well as monitoring security exchanges, brokerage firms, transfer agents, clearing agencies, and securities self regulatory organisations such as the New York Stock Exchange<sup>6</sup>. 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 . 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<sup>7</sup> that ‘[f]raud and manipulation involving bitcoin traded in interstate commerce are appropriately within the purview of the CFTC’. 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*.

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. 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 Bitcoin are found not to carry a right to a declared dividend, a right to vote on an issuer’s affairs or conduct and any kind of right to participate in the economic success of a juridical entity. In addition, Bitcoin neither constitutes a note nor a

---

<sup>6</sup>Investor Bulletin: Private Placements Under Regulation D, Securities and Exchange Commission, 2014. Available [https://www.sec.gov/oia/investor-alerts-bulletins/ib\\_privateplacements.html](https://www.sec.gov/oia/investor-alerts-bulletins/ib_privateplacements.html)

<sup>7</sup>Clayton, Jay. 2017. “Statement on Cryptocurrencies and Initial Coin Offerings.” Public Statements. Last modified December 11, 2017. Available [here](#)



bond, as transactions for or in Bitcoins do not themselves result in any continuing obligation of one party to pay another. Instead, there is a possibility that Bitcoin could be representative of an investment contract. In the landmark Supreme Court case *SEC v. Shavers* [*Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust*, Civil Action No. Civil Action No. 4:13-CV-416], 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. This has incorrectly led to the assumption that Bitcoins are securities and therefore subject to SEC regulations. In another landmark Supreme Court case, *SEC v. Howey* [328 U.S. 293 (1946)], 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. 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. As such, ICOs enable investors to exchange currency such as U.S. dollars or cryptocurrencies in return for a digital asset labelled as a coin or token. An ICO bears resemblance to a security or a security offering ‘when the promoters of these offerings emphasise the secondary market trading potential of these tokens. In conducting a ‘Howey Test’, the SEC found that the investment of money element is usually ‘satisfied in an offer and sale of’ Bitcoin<sup>8</sup>, as is the common enterprise feature ([90]). 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. 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. 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. Third, and repeatedly, 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 indicative of the fact that the SEA framework is not a good fit.

In October 2019, the SEC, the CFTC and FinCEN issued a joint statement stressing that all

---

<sup>8</sup>Framework for ‘Investment Contract’ Analysis of Digital Assets, SEC, Securities and Exchange Commission, 2019.



companies ‘with registered digital assets’ are subject to AML regulations under the BSA. Previously, trading and investing in digital assets had fallen into a regulatory grey area as to which existing laws apply. However, the agencies clarified that regulations applied irrespective of whether broker-dealers were handling securities or commodities. 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 certain 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]’.

Second, unlike an IPO where investors buy shares of a company, the tokens acquired in an ICO do not signify ownership in a company ([103]). 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, life-cycle of the project, other legal terms and conditions, and more’ ([101]). However, white papers tend to be significantly less detailed than a prospectus and do not ‘adhere to any specified guidelines’. This has presented to criminals the possibility of raising real money without offering anything meaningful in exchange and without preparing any complex documentations. With this money, it is possible to engage in money laundering or terrorist financing.

### 3.4. *The IRS: 2014 Guidance*

In 2014, the IRS issued a Guidance stipulating that Bitcoin is considered a property for federal tax purposes<sup>9</sup>. 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. 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. 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’. 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’. 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

---

<sup>9</sup>Internal Revenue Service. 2014. “Internal Revenue Bulletin: 2014-16.” IRB. Last modified April 14, 2014. [https://www.irs.gov/irb/2014-16\\_IRBNOT-2014-21](https://www.irs.gov/irb/2014-16_IRBNOT-2014-21)

property that is not a capital asset, which includes inventory and other property held mainly for sale to customers in a trade or business.

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 ([75]). However, Bitcoin does not necessitate such an agreement. Instead, '[Bitcoin] merely relies on the fulfilment of technological requirements, namely the use of the correct private and public key'. Property law also assures that when a mistake has occurred, the transfer is voidable. 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. In this way, Bitcoin 'does not take into account mistakes, fraud, or improper threats'. 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. 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 directly purchase goods and services. The IRS' Guidance 'sent a panic through the industry' as users were primarily using Bitcoin as a payment mechanism and feared 'labelling virtual currencies as property signalled the death [of] Bitcoin's chance at becoming a staple digital currency and even potential rival to conventional currency' ([76]). 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 'from [a] friend's wallet' or one 'found on the ground' ([76]). However with Bitcoin, using a coin purchased at \$10 will have a different, less favourable tax consequence than using a coin purchased at \$50.

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' ([84]). 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.

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 ([77]). This is complicated by

the fact that Bitcoin is pseudo-anonymous, which exacerbates the IRS' ability to determine 'what gains or losses are realised from the Bitcoins'. Thirdly, the extreme fluctuation in the price of Bitcoin obscures users' ability to determine its fair market value and basis ([77]). This is exacerbated by the fact that users can purchase bitcoins from different vendors at different rates and at different times. This confusion has emboldened some criminals from under-reporting or otherwise manipulating 'the amount of Bitcoin that is eventually reported to the IRS', enabling them to evade taxes and hide a portion of income that can be used for money laundering or terrorist financing ([77]). 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. 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.

### *3.5. The Potential for Private Sector Self-Regulation*

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, we 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, or transact in 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.<sup>10</sup> 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). 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 ATT, 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, we 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

---

<sup>10</sup>Available at: <https://www.w3.org/>

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 centralised and standardised 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, standardisation would mitigate the legal and jurisdictional mosaic of international perspectives on Bitcoin use and regulation. In this paper we primarily limit our considerations to the US Context but it is important to note that the European Union has made progress in this space with the Fifth Anti-Money Laundering Directive (5MLD).<sup>11</sup> It is proposed as a and object of future research to investigate exclusively the European Union’s and specifically the European Central Bank’s regulatory response to cryptocurrencies and Bitcoin.

However, one major limitation to the W3C 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’ ([65]). 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 ([65]).

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 3 depicts this dynamic.

**Insert Figure 3 about here**

---

<sup>11</sup>Please see [https://www.europarl.europa.eu/cmsdata/150761/TAX3\\_Study\\_on\\_cryptocurrencies\\_and\\_blockchain.pdf](https://www.europarl.europa.eu/cmsdata/150761/TAX3_Study_on_cryptocurrencies_and_blockchain.pdf) for further information on the 5MLD.

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 incentivise the W3C to ensure regulation is up to par.

A potential ‘real-world’ parallel for this framework would be the relationship between the International Civil Aviation Organisation (ICAO) and the Federal Aviation Administration (FAA). The ICAO is a specialised agency of the United Nations, founded in 1944 to create standards and global norms to ensure ‘a safe, efficient, secure, economically sustainable and environmentally responsible civil aviation sector’ (International Civil Aviation Organisation)<sup>12</sup>. Such standards range from environmental protection<sup>13</sup>, such as using environmentally sustainable aviation fuel, to aviation security, which pertains to runway safety and unauthorised takeover of aircraft as in terrorist attacks, for example (International Civil Aviation Organisation)<sup>14</sup>.

The FAA is a subsidiary of the U.S. Department of Transportation and is responsible for enforcing aviation regulations and standards in the U.S. among private sector entities regarding aircraft, airport, and runway safety. Because the U.S. is a signatory to the ICAO, the FAA must ensure its regulations are in compliance with the regulations and standards of the ICAO. The ICAO takes the stance that its ‘role is not to penalise and blame countries when they may demonstrate shortcomings in the carrying out of an international responsibility, but rather to coordinate or provide assistance and capacity-building to help them do so more effectively in the future’ (International Civil Aviation Organisation). As such, in the event of an infraction, the U.S. and the FAA would generally be subject to public ‘naming-and-shaming’ or, in certain circumstances, may face sanctions ‘in the form of suspension of voting powers in the Assembly and in the Council’ (International Civil Avi-

---

<sup>12</sup><https://www.icao.int/about-icao/Pages/default.aspx>

<sup>13</sup>Further information surrounding issues with regards to energy and environmental issues that must be considered by cryptocurrency enthusiasts can be found at [46]

<sup>14</sup><https://www.icao.int/about-icao/Pages/default.aspx>

ation Organisation)<sup>15</sup>. In this way, the FAA is responsible for rectifying and punishing instances of non-compliance. The FAA has an incentive to do this, however, as the FAA and the private sector companies it oversees are granted a significant amount of legitimacy within the international community for upholding ICAO standards.

In parallel to the Bitcoin framework, the W3C is similar to the ICAO in the sense that they are both international bodies that establish guidelines and standards for a community. State governments would act like the FAA and be responsible for prosecuting any malicious behaviour associated with Bitcoin companies or users. Where the discussed framework diverges from this parallel slightly is that the W3C (international entity) must ultimately answer to state governments, whereas the FAA (state government body), answers to the standards established by the ICAO (international entity). 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]' ([92]). 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' ([91]). 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. Under this framework, and considering the AML/CFT protections covered, 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 Store and run on Apple products. In return, companies would be required to

---

<sup>15</sup>See [here](#) and the full statement of the standing rules and procedures of the ICAO [here](#)

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 Apple Store for non-compliance issues. This followed Google's temporary move to remove MetaMask, the Android equivalent of a bitcoin wallet, from Google Play. 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. 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 'red-list' of the hashes [cryptographic algorithms] which identify wallets that have been involved in criminal activities. Once on the red list, W3C could prohibit Bitcoin companies from carrying out transactions connected with these wallets. This would prevent individuals from donating bitcoins to a red-listed wallet associated with a terrorist group, for example. Such a refusal would make the value of the coins in criminal wallets practically worthless, since no transactions can be conducted with them. 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 organisations, 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.

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, which undermines Bitcoin’s attractive pseudo-anonymous quality. However in this discussed framework, 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. 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 incentivised to register, competition for fair pricing and services increases, which benefits users. Secondly, 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 those in areas where the formal banking sector is plagued by corruption or simply nonexistent altogether – by introducing a new, acceptable payment system. Finally, 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.

**Insert Table 1 about here**

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’. 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. Table 1 summarises the main points analysed in this section.

#### **4. Discussion**

When analysing 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, one could argue that Bitcoin should be considered a new type of technology under the burgeoning FinTech industry. As such, regulation should rest with private sector technology companies, namely the W3C in a three-tiered framework.

There are several significant limitations to this study: First, and most importantly, this framework could be rendered obsolete if the price of Bitcoin were to stabilise dramatically and consistently. Of the four existing legal frameworks analysed in this paper, Bitcoin least problematically fits into the framework proposed by the CFTC. If the price of Bitcoin stabilises, 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 stabilise 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.

Additional limitations include achieving international consensus on self-regulation led by the private sector will be extremely difficult. It will most likely 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 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. 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. This study would benefit from more research to determine specific mechanisms besides red-listing to better detect and prevent terrorist financing, money laundering, and other illicit activities.

## 5. Concluding Comments

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 conceptualise 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 2014 Guidance – it is clear that none truly account for the unique properties of Bitcoin nor do they effectively address AML/CFT concerns.

This research 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 technology companies. 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. Therefore, further research is needed to see how best to integrate the emerging global regulatory standards of the United States, the European Union and China as they vie for universal, or near universal, adoption. 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

- [1] Tobias Adrian and Tommaso Mancini Griffoli. The rise of digital money. *International Monetary Fund*, 2019.
- [2] M. Akhtaruzzaman, A. Sensoy, and S. Corbet. The influence of bitcoin on portfolio diversification and design. *Finance Research Letters*, 2019.
- [3] E. Akyildirim, S. Corbet, D. Cumming, B. Lucey, and A. Sensoy. Riding the wave of crypto-exuberance: The potential misuse of corporate blockchain announcements. *Technological Forecasting and Social Change*, 159, 2020.
- [4] E. Akyildirim, S. Corbet, P. Katsiampa, N. Kellard, and A. Sensoy. The development of bitcoin futures: Exploring the interactions between cryptocurrency derivatives. *Finance Research Letters*, 2019.
- [5] E. Akyildirim, S. Corbet, D.K. Nguyen, and A. Sensoy. Regulatory changes and long-run relationships of the emu sovereign debt markets: Implications for future policy framework. *International Review of Law and Economics*, 63, 2020.
- [6] A.F. Aysan, E. Demir, G. Gozgor, and C.K.M. Lau. Effects of the geopolitical risks on bitcoin returns and volatility. *Research in International Business and Finance*, 47:511–518, 2019.

- [7] Dirk G Baur, Kihoon Hong, and Adrian D Lee. Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money*, 54:177–189, 2018.
- [8] P. Bedi and T. Nashier. On the investment credentials of bitcoin: A cross-currency perspective. *Research in International Business and Finance*, 51, 2020.
- [9] C. Beneki, A. Koulis, N.A. Kyriazis, and S. Papadamou. Investigating volatility transmission and hedging properties between bitcoin and ethereum. *Research in International Business and Finance*, 48:219–227, 2019.
- [10] B.M. Blau. Price dynamics and speculative trading in bitcoin. *Research in International Business and Finance*, 41:493–499, 2017.
- [11] B.M. Blau. Price dynamics and speculative trading in bitcoin. *Research in International Business and Finance*, 43:15–21, 2018.
- [12] Rhys Bollen. The legal status of online currencies: are bitcoins the future? *Journal of Banking and Finance Law and Practice*, 2013.
- [13] Alan Brill and Lonnie Keene. Cryptocurrencies: The next generation of terrorist financing? *Defence against terrorism review*, 6(1):7–30, 2014.
- [14] Danton Bryans. Bitcoin and money laundering: mining for an effective solution. *Ind. LJ*, 89:441, 2014.
- [15] G.M. Caporale, L. Gil-Alana, and A. Plastun. Persistence in the cryptocurrency market. *Research in International Business and Finance*, 46:141–148, 2018.
- [16] G.M. Caporale and T. Zekokh. Modelling volatility of cryptocurrencies using markov-switching garch models. *Research in International Business and Finance*, 48:143–155, 2019.
- [17] Jon Carrick. Bitcoin as a complement to emerging market currencies. *Emerging Markets Finance and Trade*, 52(10):2321–2334, 2016.
- [18] V. Celeste, S. Corbet, and C. Gurdgiev. Fractal dynamics and wavelet analysis: Deep volatility and return properties of bitcoin, ethereum and ripple. *Quarterly Review of Economics and Finance*, 76:310–324, 2020.
- [19] Eric D Chason. How bitcoin functions as property law. *Seton Hall Law Review*, 49:129, 2018.
- [20] J. Chu, S. Chan, and Y. Zhang. High frequency momentum trading with cryptocurrencies. *Research in International Business and Finance*, 52, 2020.
- [21] Jeffrey Chu, Saralees Nadarajah, and Stephen Chan. Statistical analysis of the exchange rate of bitcoin. *PloS one*, 10(7):e0133678, 2015.
- [22] Theodore H Cohn. *Global political economy*. Routledge, 2015.
- [23] T. Conlon, S. Corbet, and R.J. McGee. Are cryptocurrencies a safe haven for equity markets? an international perspective from the covid-19 pandemic. *Research in International Business and Finance*, 54, 2020.
- [24] Thomas Conlon and Richard McGee. Safe haven or risky hazard? bitcoin during the covid-19 bear market. *Finance Research Letters*, page 101607, 2020.
- [25] S. Corbet, D.J. Cumming, B.M. Lucey, M. Peat, and S.A. Vigne. The destabilising effects of cryptocurrency cyber-criminality. *Economics Letters*, 191, 2020.
- [26] S. Corbet, J.J. Dunne, and C. Larkin. Quantitative easing announcements and high-frequency stock market volatility: Evidence from the united states. *Research in International Business and Finance*, 48:321–334, 2019.
- [27] S. Corbet, V. Eraslan, B. Lucey, and A. Sensoy. The effectiveness of technical trading rules in cryptocurrency markets. *Finance Research Letters*, 31:32–37, 2019.

- [28] S. Corbet, Y.G. Hou, Y. Hu, C. Larkin, and L. Oxley. Any port in a storm: Cryptocurrency safe-havens during the COVID-19 pandemic. *Economics Letters*, 194, 2020.
- [29] S. Corbet, Y.G. Hou, Y. Hu, L. Oxley, and D. Xu. Pandemic-related financial market volatility spillovers: Evidence from the chinese covid-19 epicentre. *International Review of Economics and Finance*, 71:55–81, 2021.
- [30] S. Corbet, C. Larkin, B. Lucey, A. Meegan, and L. Yarovaya. Cryptocurrency reaction to fomc announcements: Evidence of heterogeneity based on blockchain stack position. *Journal of Financial Stability*, 46, 2020.
- [31] S. Corbet, C. Larkin, B. Lucey, and L. Yarovaya. Kodakcoin: a blockchain revolution or exploiting a potential cryptocurrency bubble? *Applied Economics Letters*, 27(7):518–524, 2020.
- [32] S. Corbet, C. Larkin, B.M. Lucey, A. Meegan, and L. Yarovaya. The impact of macroeconomic news on bitcoin returns. *European Journal of Finance*, 2020.
- [33] S. Corbet, B. Lucey, M. Peat, and S. Vigne. Bitcoin futures—what use are they? *Economics Letters*, 172:23–27, 2018.
- [34] S. Corbet, B. Lucey, M. Peat, and S. Vigne. What sort of asset? bitcoin analysed. *Lecture Notes in Business Information Processing*, 345:52–65, 2019.
- [35] S. Corbet, B. Lucey, and L. Yarovaya. Datestamping the bitcoin and ethereum bubbles. *Finance Research Letters*, 26:81–88, 2018.
- [36] S. Corbet, G. McHugh, and A. Meegan. The influence of central bank monetary policy announcements on cryptocurrency return volatility. *Investment Management and Financial Innovations*, 14(4):60–72, 2017.
- [37] S. Corbet, A. Meegan, C. Larkin, B. Lucey, and L. Yarovaya. Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Economics Letters*, 165:28–34, 2018.
- [38] Shaen Corbet. *Evaluating a decade of cryptocurrency development: Navigating financial progress through technological and regulatory ambiguity*, pages 185 – 196. De Gruyter, Berlin, Boston, 2020.
- [39] Shaen Corbet and Douglas J Cumming. The Wild West of ICOs. *Cryptocurrency and Blockchain Technology*, Walter de Gruyter GmbH & Co KG, 1:113–130, 2020.
- [40] Shaen Corbet, Greg Hou, Yang Hu, and Les Oxley. The influence of the covid-19 pandemic on asset-price discovery: Testing the case of chinese informational asymmetry. *Available at SSRN 3623274*, 2020.
- [41] Shaen Corbet, Yang Hou, Yang Hu, Brian Lucey, and Les Oxley. Aye corona! the contagion effects of being named corona during the covid-19 pandemic. *Finance Research Letters*, page 101591, 2020.
- [42] Shaen Corbet, Charles Larkin, and Brian Lucey. The contagion effects of the covid-19 pandemic: Evidence from gold and cryptocurrencies. *Finance Research Letters*, page 101554, 2020.
- [43] Shaen Corbet and Brian Lucey. *An analysis of the development of cryptocurrency research*, pages 23 – 54. De Gruyter, Berlin, Boston, 2020.
- [44] Shaen Corbet, Brian Lucey, Andrew Urquhart, and Larisa Yarovaya. Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis*, 62:182–199, 2019.
- [45] Shaen Corbet, Andrew Urquhart, and Larisa Yarovaya. *Cryptocurrency and Blockchain Technology*. De Gruyter, Berlin, Boston, 2020.
- [46] Shaen Corbet and Larisa Yarovaya. *The environmental effects of cryptocurrencies*, pages 149 – 184. De Gruyter, Berlin, Boston, 2020.
- [47] Cynthia Dion-Schwarz, David Manheim, and Patrick B Johnston. *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. Rand Corporation, 2019.

- [48] A. Eross, F. McGroarty, A. Urquhart, and S. Wolfe. The intraday dynamics of bitcoin. *Research in International Business and Finance*, 49:71–81, 2019.
- [49] M. Fakhfekh and A. Jeribi. Volatility dynamics of crypto-currencies’ returns: Evidence from asymmetric and long memory garch models. *Research in International Business and Finance*, 51, 2020.
- [50] A.P. Fassas, S. Papadamou, and A. Koulis. Price discovery in bitcoin futures. *Research in International Business and Finance*, 52, 2020.
- [51] A. Flori. News and subjective beliefs: A bayesian approach to bitcoin investments. *Research in International Business and Finance*, 50:336–356, 2019.
- [52] David Fox and Sarah Green. Cryptocurrencies in public and private law. 2019.
- [53] Michael Freeman. The sources of terrorist financing: Theory and typology. *Studies in Conflict & Terrorism*, 34(6):461–475, 2011.
- [54] L. Garcia-Jorcano and S. Benito. Studying the properties of the bitcoin as a diversifying and hedging asset through a copula analysis: Constant and time-varying. *Research in International Business and Finance*, 54, 2020.
- [55] L.A. Gil-Alana, E.J.A. Abakah, and M.F.R. Rojo. Cryptocurrencies and stock market indices. are they related? *Research in International Business and Finance*, 51, 2020.
- [56] Simon Gleeson. The legal concept of money. 2018.
- [57] J.W. Goodell. Comparing normative institutionalism with intended rationality in cultural-finance research. *International Review of Financial Analysis*, 62:124–134, 2019.
- [58] J.W. Goodell. Covid-19 and finance: Agendas for future research. *Finance Research Letters*, 35, 2020.
- [59] J.W. Goodell and S. Goutte. Co-movement of covid-19 and bitcoin: Evidence from wavelet coherence analysis. *Finance Research Letters*, 2020.
- [60] J.W. Goodell and T.L.D. Huynh. Did congress trade ahead? considering the reaction of us industries to covid-19. *Finance Research Letters*, 36, 2020.
- [61] J.W. Goodell, R.J. McGee, and F. McGroarty. Election uncertainty, economic policy uncertainty and financial market uncertainty: A prediction market analysis. *Journal of Banking and Finance*, 110, 2020.
- [62] J.W. Goodell, F. McGroarty, and A. Urquhart. Political uncertainty and the 2012 us presidential election: A coin-tegration study of prediction markets, polls and a stand-out expert. *International Review of Financial Analysis*, 42:162–171, 2015.
- [63] Reuben Grinberg. Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal*, 4:159, 2012.
- [64] Marc Gronwald. Is bitcoin a commodity? on price jumps, demand shocks, and certainty of supply. *Journal of International Money and Finance*, 97:86–92, 2019.
- [65] Andres Guadamuz and Christopher Marsden. Blockchains and bitcoin: Regulatory responses to cryptocurrencies. *First Monday*, 20(12-7), 2015.
- [66] Y. Hu, X. Li, and D. Shen. Attention allocation and international stock return comovement: Evidence from the bitcoin market. *Research in International Business and Finance*, 54, 2020.
- [67] Thomas A. Hulme. *The ethical and legal aspects of blockchain technology and cryptoassets*, pages 131 – 148. De Gruyter, Berlin, Boston, 2020.
- [68] V. Kallinterakis and Y. Wang. Do investors herd in cryptocurrencies – and why? *Research in International Business and Finance*, 50:240–245, 2019.

- [69] Nikolei Kaplanov. Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Loyola Consumer Law Review*, 25:111, 2012.
- [70] P. Katsiampa, S. Corbet, and B. Lucey. High frequency volatility co-movements in cryptocurrency markets. *Journal of International Financial Markets, Institutions and Money*, 62:35–52, 2019.
- [71] P. Katsiampa, S. Corbet, and B. Lucey. Volatility spillover effects in leading cryptocurrencies: A bekk-mgarch analysis. *Finance Research Letters*, 29:68–74, 2019.
- [72] A. Klarin. The decade-long cryptocurrencies and the blockchain rollercoaster: Mapping the intellectual structure and charting future directions. *Research in International Business and Finance*, 51, 2020.
- [73] N. Kyriazis, S. Papadamou, and S. Corbet. A systematic review of the bubble dynamics of cryptocurrency prices. *Research in International Business and Finance*, 54, 2020.
- [74] S. Lee, N.E. Meslmani, and L.N. Switzer. Pricing efficiency and arbitrage in the bitcoin spot and futures markets. *Research in International Business and Finance*, 53, 2020.
- [75] Matthias Lehmann. Who owns bitcoin: Private law facing the blockchain. *Minnesota Journal of Science & Technology*, 21:93, 2019.
- [76] Stephanie A Lemchuk. Virtual whats: Defining virtual currencies in the face of conflicting regulatory guidances. *Cardozo Public Law Policy & Ethics Journal*, 15:319, 2016.
- [77] Allison M Lovell. Avoiding liability: Changing the regulatory structure of cryptocurrencies to better ensure legal use. *Iowa Law Review*, 104:927, 2018.
- [78] Kelvin FK Low and Ernie GS Teo. Bitcoins and other cryptocurrencies as property? *Law, Innovation and Technology*, 9(2):235–268, 2017.
- [79] D. Ma and H. Tanizaki. The day-of-the-week effect on bitcoin return and volatility. *Research in International Business and Finance*, 49:127–136, 2019.
- [80] Tara Mandjee. Bitcoin, its legal classification and its regulatory framework. *Journal of Business & Securities Law*, 15(2):157, 2015.
- [81] Bennett T McCallum. The bitcoin revolution. *Cato Journal*, 35:347, 2015.
- [82] W. Mensi, M. Ur Rehman, D. Maitra, K. Hamed Al-Yahyaee, and A. Sensoy. Does bitcoin co-move and share risk with sukuk and world and regional islamic stock markets? evidence using a time-frequency approach. *Research in International Business and Finance*, 53, 2020.
- [83] I. Merediz-Solá and A.F. Bariviera. A bibliometric analysis of bitcoin scientific production. *Research in International Business and Finance*, 50:294–305, 2019.
- [84] Nicole Mirjanich. Digital money: Bitcoin’s financial and tax future despite regulatory uncertainty. *DePaul Law Review*, 64:213, 2014.
- [85] P. Nadler and Y. Guo. The fair value of a token: How do markets price cryptocurrencies? *Research in International Business and Finance*, 52, 2020.
- [86] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.
- [87] T.V.H. Nguyen, B.T. Nguyen, K.S. Nguyen, and H. Pham. Asymmetric monetary policy effects on cryptocurrency markets. *Research in International Business and Finance*, 48:335–339, 2019.
- [88] T.V.H. Nguyen, B.T. Nguyen, T.C. Nguyen, and Q.Q. Nguyen. Bitcoin return: Impacts from the introduction of new altcoins. *Research in International Business and Finance*, 48:420–425, 2019.

- [89] Lam Pak Nian and David Lee Kuo Chuen. Introduction to bitcoin. In *Handbook of digital currency*, pages 5–30. Elsevier, 2015.
- [90] Hester M. Peirce. How we howey.
- [91] Thomas Philippon. The fintech opportunity. Technical report, National Bureau of Economic Research, 2016.
- [92] Thomas Puschmann. Fintech. *Business & Information Systems Engineering*, 59(1):69–76, 2017.
- [93] Perri Reynolds and Angela SM Irwin. Tracking digital footprints: anonymity within the bitcoin system. *Journal of Money Laundering Control*, 2017.
- [94] Linda M Schilling and Harald Uhlig. Currency substitution under transaction costs. In *AEA Papers and Proceedings*, volume 109, pages 83–87, 2019.
- [95] Syed Jawad Hussain Shahzad, Elie Bouri, David Roubaud, Ladislav Kristoufek, and Brian Lucey. Is bitcoin a better safe-haven investment than gold and commodities? *International Review of Financial Analysis*, 63:322–330, 2019.
- [96] Y. Shi, A.K. Tiwari, G. Gozgor, and Z. Lu. Correlations among cryptocurrencies: Evidence from multivariate factor stochastic volatility model. *Research in International Business and Finance*, 53, 2020.
- [97] I.M. Sifat, A. Mohamad, and M.S.B. Mohamed Shariff. Lead-lag relationship between bitcoin and ethereum: Evidence from hourly and daily data. *Research in International Business and Finance*, 50:306–321, 2019.
- [98] Nicole D Swartz. Bursting the bitcoin bubble: The case to regulate digital currency as a security or commodity. *Tulane Journal of Technology & Intellectual Property*, 17:319, 2014.
- [99] E. Symitsi and K.J. Chalvatzis. The economic value of bitcoin: A portfolio analysis of currencies, gold, oil and stocks. *Research in International Business and Finance*, 48:97–110, 2019.
- [100] Efthymia Symitsi and Konstantinos J Chalvatzis. The economic value of bitcoin: A portfolio analysis of currencies, gold, oil and stocks. *Research in International Business and Finance*, 48:97–110, 2019.
- [101] Milind Tiwari, Adrian Gepp, and Kuldeep Kumar. The future of raising finance-a new opportunity to commit fraud: a review of initial coin offering (icos) scams. *Crime, Law and Social Change*, pages 1–25, 2019.
- [102] Jonathan B Turpin. Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework. *Indiana Journal of Global Legal Studies*, 21:335, 2014.
- [103] AV Vorobyev. Ico as economic security threat. possible risks analysis. experience of foreign states. *KnE Social Sciences*, pages 208–214, 2018.
- [104] P. Wang, X. Li, D. Shen, and W. Zhang. How does economic policy uncertainty affect the bitcoin market? *Research in International Business and Finance*, 53, 2020.
- [105] Scott A Wiseman. Property or currency: The tax dilemma behind bitcoin. *Utah L. Rev.*, page 417, 2016.
- [106] David Yermack. Is bitcoin a real currency? an economic appraisal. In *Handbook of digital currency*, pages 31–43. Elsevier, 2015.
- [107] F.N. Zargar and D. Kumar. Informational inefficiency of bitcoin: A study based on high-frequency data. *Research in International Business and Finance*, 47:344–353, 2019.

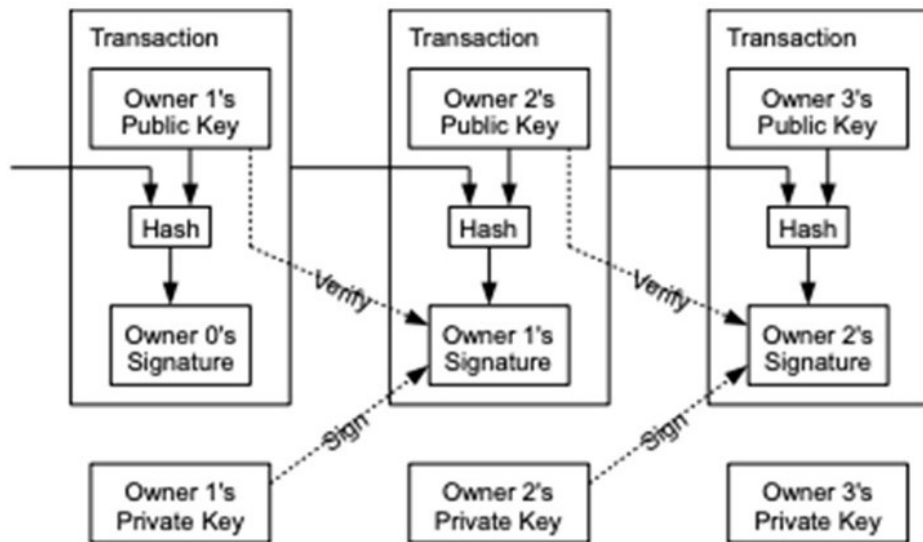
Table 1: Evaluating Regulatory Frameworks

Frameworks	FinCEN: BSA	CFTC: CEA	SEC: Securities Act of 1933 / SEA	IRS: Guidance
<i>Bitcoin properties</i>	<p>Bitcoin is a currency</p> <p>Is not an effective medium of exchange, a unit of account, or store of value</p> <p>Undermined by 21 million cap and extreme price fluctuations</p> <p>Bitcoin is still not accepted at some major retailers</p>	<p>Bitcoin is a commodity</p> <p>Not federally regulated, has a finite supply, can be traded</p> <p>Does not consistently act like a hedge or safe haven</p>	<p>Bitcoin is a security</p> <p>Bitcoin does not fit the definition of securities such as stocks, bonds, notes and investment contracts</p> <p>An ICO is similar to an investment contract, but in most circumstances fails the Howey Test</p>	<p>Bitcoin is a property</p> <p>Bitcoin properties complicate several factors of property law including making agreements on transfers and voiding fraudulent or mistaken transfers</p>
<i>AML/CFT concerns</i>	<p>CTRs and SARs can deter criminals</p> <p>BSA applies to money transmitters, not users</p> <p>Criminals can evade reporting requirements by transacting in smaller amounts</p>	<p>Subject to the BSA, the same loopholes apply</p> <p>CFTC does not have jurisdiction over Bitcoin exchanges for cash</p>	<p>Subject to the BSA, the same loopholes apply</p> <p>Private and limited offerings do not need to register with the SEC</p>	<p>Does not directly address AML/CFT concerns despite reporting requirements</p> <p>Price fluctuations may cause under-reporting</p> <p>Relies on self-reporting, which can be abused by criminals</p>

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

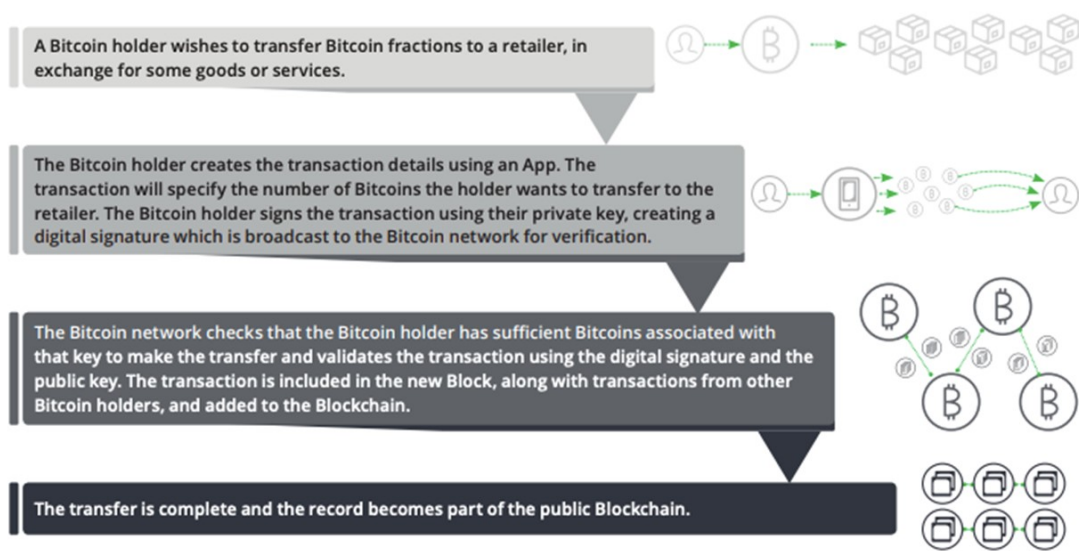


Figure 1: Trajectory of a Bitcoin Transaction



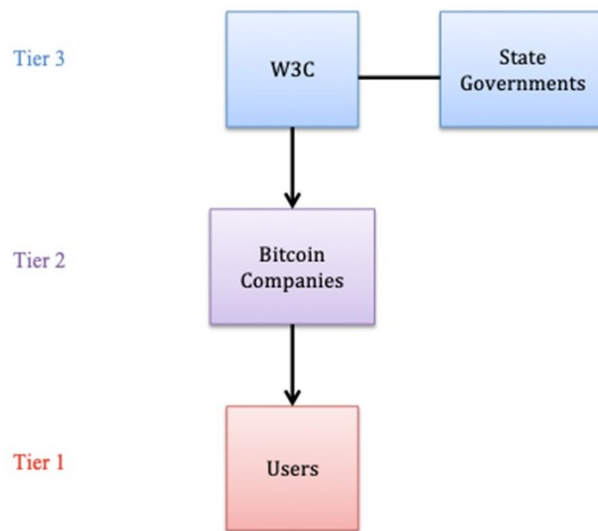
Note: The above figures depicts as to how a bitcoin transaction works using the public and private keys ([86]).

Figure 2: Illustration of the Bitcoin Mining and Verification Process



Note: The above figure depicts the mining and verification processes (Uhl, Robert, Amy Steele, Ivan O'Donnell, Doug Zercoe, and Peter Taylor. 2019. Classification of Cryptocurrency Holdings, New York, NY: Deloitte. Available [here](#)).

Figure 3: Flowchart for a Three-Tiered Framework for Bitcoin Regulation



Note: The above figure depicts the dynamics of W3C as 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.