Intellectual Property Brief

Volume 9 | Issue 2 Article 2

2018

U.S. Regulation of Blockchain Currencies: A Policy Overview

Averie Brookes
Sandra Day O'Connor College of Law

U.S. Regulation of Blockchain Currencies: A Policy Overview

U.S. REGULATION OF BLOCKCHAIN CURRENCIES: A POLICY OVERVIEW

Averie Brookes[1]

ABSTRACT

With its increasing significance in real-world financial transactions, blockchain currency has risen to a level of significance that regulators and policymakers can no longer ignore. Cryptocurrency has developed so fast. It is outpacing the regulatory and legislative developments necessary to address the issues that it has stirred up. Although cryptocurrency regulations have been in place for the past several years, already, lawmakers have struggled to keep up with the increasing popularity and technical complexity of cryptocurrency market activity.

This paper is not intended to be an extensive guide to the software and programming innovations that gave rise to this new financial technology. Rather, the purpose of this analysis is to clarify how virtual currency – one that has no real-world legal tender status like "fiat" currency issued by a central, sovereign authority – operating on decentralized, peer-to-peer networks should and will be integrated into existing financial regulatory systems. This analysis will focus on the U.S. regulatory system, although financial regulators around the world confront similar issues.

[1] Averie Brookes is a recent graduate of Sandra Day O'Connor College of Law, at Arizona State University. Her emphasis of study was in corporate and business law. Prior to attending law school, she worked as a forensic account for a major financial institution. She developed an interest in cryptocurrency with the advent of Bitcoin. As an early adopter of the blockchain technology, she studied, analyzed, and invested in various cryptocurrencies. Her unique background enables her to marry a traditional monetary analysis with the emerging and ever-changing technology and legal basis for the future of cryptocurrencies.

TABLE OF CONTENTS

I. INTRODUCTION

Virtual (or crypto) currencies operating on blockchain technology are creating an entirely new financial service and commodity exchange market that policymakers and laypeople alike may find difficult to integrate into traditional beliefs about how currency and related securities operate in our daily lives. Over the decade since its invention, blockchain currency has evolved from a fringe internet phenomenon to a new type of commodity that is turning traditional financial markets on their heads.

In the cryptocurrency world, things move fast. Bitcoin, the world's first fully decentralized digital currency, now exceeds the Gross Domestic Product ("GDP") of some small nations and is attracting the attention of serious investors and venture capitalists.[2] Until quite recently, however, blockchain currencies were largely unregulated, and developers were left to their own devices. While this lack of regulation has fostered important social and technological innovations based on the blockchain model, it has also opened the door for criminal or fraudulent activities. To ensure that blockchain currencies are used in a manner that preserves the substantial benefits of this groundbreaking technology, regulators should take a firm but cautious approach to controlling certain activities in virtual currency markets.

This paper begins with a brief exploration of blockchain technology and virtual currencies, and how these new inventions differ from our current understanding of money and financial markets. It continues with an explanation of the current uses and benefits of blockchain currencies, as well as the issues and concerns created by this new technology. The article then discusses some of the major issues impacting cryptocurrency markets in the United States at present, which have arisen concurrently with increased mainstream adoption. The analysis continues with an overview of the current regulatory programs that address blockchain currencies in their various functions, including both federal and state actions regarding cryptocurrencies. The narrative concludes with an overview of self-regulation and corporate policies that have been developed to address some of the problems facing virtual currency activities in an unregulated environment.

II. A BRIEF PRIMER ON BLOCKCHAIN TECHNOLOGY & VIRTUAL CURRENCY

Blockchain currency was invented in 2008 by an as-of-yet unidentified individual or group known as Satoshi Nakamoto – a pseudonym for the

[2] *See generally* Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* 1 (2016) https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv2_0.pdf (indicating that, as of 2016, the total Bitcoin economy was worth an estimated $6.4 billion).

inventor of Bitcoin, the world's first virtual currency.[3] Virtual blockchain currencies are not simply electronic versions of real-world legal tender. Rather, they exist with no central bank issuing and controlling the money supply, no direct regulation of transactions or related securities exchanges, and no denomination in fiat currency.[4] To fully understand how blockchain technology functions to create and support virtual currency, it is necessary to clarify how these technologies operate, their current use and function, and how they are likely to impact future financial transactions.

A. Blockchain Technology

Blockchain is a revolutionary technology that has the potential to change not only currency and financial markets but perhaps even the Internet itself. At its core, blockchain is a system for solving complex problems. More specifically, blockchain is a ledger of transactions, with each "block" representing a single piece of data that is recorded chronologically in a "chain." The blockchain ledger is unique because it operates without direct management from a centralized controlling organization. Furthermore, no single, centralized location – such as a server, cloud, or file room – houses the blockchain ledger. This lack of central location and control is characteristic of blockchain technology, which is typically defined as "a decentralized peer-to-peer network that maintains a public, or private, ledger of transactions."[5]

Decentralization is key to understanding blockchain technology because it inherently requires a network of users all running identical software applications that operate under the same set of rules, or "protocol." Every single user maintains a copy of the blockchain ledger on his or her computer. The computers in the network must come to a consensus in order to make changes to the ledger. Specifically, the majority of the network must run the changes through the protocol and agree that they are appropriate. This consensus serves to validate the proposed change to the blockchain before it is made. In short, blockchain technology is a new way to collect, store, and validate complex data in a manner that does not require centralized management. Rather, the data collection and validation occur semi-autonomously through a network of users independently running identical software that reviews data for compliance with ledger rules. While blockchains have many diverse potential applications, the first, and still most important, application of the blockchain was Bitcoin.

[3] *Id.* at 5.

[4] *Id.* at 6.

[5] Shawn S. Amuial, Josias N. Dewey, & Jeffrey R. Seul, THE BLOCKCHAIN: A GUIDE FOR LEGAL & BUSINESS PROFESSIONALS 2 (2016).

B. Virtual Blockchain Currency

The first virtual currency, Bitcoin, was launched as a new protocol for blockchain technology designed to track and validate all transactions in the entire supply of the newly-created currency. Before Bitcoin's launch in 2008, all online transactions required a third-party intermediary to ensure that digital money was used only once. Independent confirmation by financial services like PayPal, Google Wallet, Apple Pay, or major credit card companies, maintains and tracks ledgers with account balances to ensure that computer-savvy users can't find a way to double-spend currency.[6] Bitcoin and similar blockchain currencies avoid third-party verification and the double spending problem by securing transactions through blockchain technology. Bitcoin's innovative software runs through the peer-to-peer network of all its users, recording all transactions identically on all computers in the entire network.[7]

Before the blockchain records a transaction, the network must first run it through verification software. Each computer reviews the entire history of transactions in the blockchain, and if the computers individually verify the proposed transaction, then the block is added to the chain and the transaction becomes part of the verified public ledger.[8] Because every transaction ever made is recorded in the blockchain, the virtual currency's software program can review this data to make sure that every coin is accounted for, thereby preventing forgery and fraud.

One particularly elegant aspect of Bitcoin's design is the linkage between the transaction verification process and how the network introduces new currency into the virtual money supply. As discussed previously, blockchain currency users form a vast peer-to-peer network where all users' computers simultaneously work to solve the increasingly complex math problems necessary to reliably verify transactions. Each separate computer's processing power is a small part of the larger infrastructure that supports the currency market. Under the Bitcoin protocol, miners supply new virtual currency whenever they successfully verify a transaction. When this occurs, the network rewards the user with a small amount of coin in a process that has become known as Bitcoin "mining." In this way, the Bitcoin protocol simultaneously creates a stable flow of currency supply and maintains a

[6] *See generally supra* note 1, at 5-6.

[7] *See generally id.* at 24-25 (Despite the hundreds of alternatives launched since 2009, Bitcoin's first-mover advantage allows it to completely dominate the blockchain cryptocurrency market. As of 2016, Bitcoin's market capitalization was about $6.4 billion -- more than seven times the market cap of Ethereum, its closest competitor, and 25 times the market share of the third-place Ripple. Additionally, Bitcoin dominates all other cryptocurrencies in other important metrics including total users, network nodes, active addresses, average transaction rate, and average value of transactions. As a result, the Bitcoin protocol is the primary example of how virtual blockchain currencies function and is the focus of much of this paper.).

[8] *See generally supra* note 4, at 3-4.

robust infrastructure for transaction verification, all without central management.[9]

On the world stage, ensuring proper currency supply and curbing market manipulation is serious business undertaken by highly trained and vetted economists and mathematicians. In traditional currency markets, a central authority creates and funds the money supply, and government agencies work together with financial service providers to verify transactions and protect against fraud. In the online world of virtual currencies, this is all done through a peer-to-peer network running complex software programs. This automation seems convenient, but the complexity of this novel technology begs the question of why people would even want to use it in the first place.

III. BLOCKCHAIN CURRENCY USES: BENEFITS, ISSUES, AND CONCERNS

Blockchain currencies are best understood not as a new type of currency, but rather, as a new way to exchange existing currencies and other items and services of value. Virtual currency transactions on the peer-to-peer network are in some ways/arguably quicker and more efficient than transactions run through third-party vendors who can take several days to perform cumbersome independent verification techniques. Eliminating the need for third-party financial vendors can bolster small businesses worldwide by lowering transaction costs, increasing worldwide access to capital, creating a new avenue for charitable giving and remittances, and spurring further innovation.[10]

The benefits of virtual currencies can be especially significant for the approximately 64% of people living in developing countries who lack reliable access to traditional financial services.[11] Bitcoin, the world's first and largest blockchain currency, offers a stable, easy-to-use currency for individuals living in nations with strict capital controls or unstable currency

[9] *See generally* Brito, *supra* note 1, at 8-9 (The Bitcoin hash algorithm is designed to become more complex over time, and awards for blockchain transaction verifications decrease as more computers are added to the network, slowly reducing the number of Bitcoins mined over time until the new currency supply approaches zero. If, on the other hand, the number of computers on the peer-to-peer network validating Blockchain transactions *decreases*, the Bitcoin hash algorithm will become easier and miners will receive new coins at greater rates. The Bitcoin protocol was designed to mimic a non-renewable natural commodity, like gold or oil. Only a limited number -- arbitrarily set at 21 million coins -- can ever be mined. Once all Bitcoins are mined, peers who commit their computers to the verification process will be awarded fees, much like third-party financial services companies today.).

[10] *See generally id.* at 13-17 (discussing research that has shown that these high fees negatively impact development in emerging economies, particularly in Africa.).

[11] *See generally id.* at 18 (providing that bitcoin is increasing in popularity across the developing world and discussing how "Bitcoin business models seek to streamline bitcoin use in developing economies.").

markets.[12] Blockchain currency access is also valuable to individuals living under oppressive regimes and others who have a legitimate interest in the privacy of their financial information, although as discussed below the degree of anonymity afforded to users of virtual currency can be problematic.

Blockchain currencies may provide valuable aid to economic development, but it is the opportunities for reduced transaction costs that have caused major investors to take notice of this new technology. Specifically, businesses using virtual currencies can minimize financial transaction fees and exchange rates, and mitigate the risk of chargeback fraud.[13] Some businesses are already offering discounts to customers paying with Bitcoin, and as consumers get more comfortable using this new technology the market is likely to increase.[14] It is improbable that Bitcoin will replace the well-known credit card companies entirely, but increased flexibility in payment options for virtual and real-world transactions offers benefits for all.

A. Current State of Cryptocurrency Markets in the U.S.

Over the past few months, cryptocurrencies have made substantial progress towards becoming mainstream financial products. There are over 110 active cryptocurrency exchanges serving millions of active users across the U.S. A growing list of retailers are accepting Bitcoin and other cryptocurrencies in exchange for goods and services. Customers of popular brands like Dell, Expedia, Microsoft, Overstock.com, PayPal, Subway, Target, and Zappos all have some ability to pay for purchases using bitcoin or other popular alternative cryptocurrencies. BitPay, one of the world's largest Bitcoin exchanges, serves over 30,000 merchants worldwide, processing about $1 million in bitcoin transactions each day. Coinbase has a similar number of business customers and has partnered with Overstock.com to increase retail use of digital currencies.

Despite this progress, cryptocurrency markets still face substantial barriers to adoption on a large scale. First and foremost, security has become a major issue. Theft and accidental loss of coins have cost the cryptocurrency markets billions over the past few years, and so far, there has been no realistic solution developed in response to this problem. Second, price volatility continues to vex investors and keep conservative financiers out of the market entirely. As more fintech entrepreneurs create cryptocurrency-based financial derivatives and regulators develop clear standards for

[12] *See, e.g.*, *id.* at 19 (discussing how Bitcoin use in Argentina has surged in recent years due to the high inflation rate of the nation's fiat currency and the strict capital controls the government has placed on the economy).

[13] *Id.* at 15-16 ("As a nonreversible payment system, Bitcoin eliminates the "friendly fraud" wrought by the misuse of consumer chargebacks, which can be very important for small businesses.").

[14] *Id.* (arguing that "the expanded choices in payment options would benefit people of all preferences.").

approval and oversight, much of this volatility is likely to subside. Finally, fraudulent activity, collusion, and price manipulation among major players in the cryptocurrency market present a major challenge to cryptocurrency investors. While federal and state financial regulators have ramped up law enforcement efforts substantially in recent months, it remains to be seen whether this issue can be addressed effectively given the inherent challenges of locating and prosecuting financial criminals.

The Securities and Exchange Commission ("SEC"), Commodity Futures Trading Commission ("CFTC"), and the Department of the Treasury are undertaking robust law enforcement measures as a signal to the cryptocurrency community at large. Many of the policies that the agencies are now actively enforcing have been in place for years. However, whether due to a lack of enforcement or general ignorance of the law, cryptocurrency investors and businesses have not taken them very seriously. Now, this is all changing. Cryptocurrencies are used to facilitate money laundering, identity theft, fraud, drug sales, tax evasion, and ransom – and there is some evidence that criminal activities are on the rise.[15]

B. Criminal Activity

While decentralization is an efficient way to verify financial transactions and useful for some legitimate purposes, this same quality makes blockchain currencies useful in criminal or fraudulent activities, such as tax evasion, money laundering, or the trade in illegal goods. Virtual currencies running on decentralized networks are designed to allow individuals to use them with a higher degree of anonymity than traditional credit card or bank transactions, which makes them useful for use in illicit or fraudulent online activity.

The blockchain displays the public keys of all users who send or receive virtual currencies. Third-party vendors like PayPal and MasterCard typically have access to far more identifying information than what is made public in the blockchain, but the time, amount, and the public keys involved in every Bitcoin transaction are publicly available.[16] Public keys - like cash - are not linked to a person's actual identity, but investigators can build this link through research. Unlike cash, however, once a public key is linked to a person's identity, investigators know all coin transactions the individual has have ever made, as this information is publicly and permanently available in the blockchain. Authorities can procure a warrant for the search of a suspected criminal's computer if there is probable cause to believe that the suspect used the machine in the commission of a crime. If the suspect stores

[15] Selva Ozelli. *Illicit Uses of Cryptocurrency Gaining Attention Around the World*, COINTELEGRAPH (Feb. 20, 2018) https://cointelegraph.com/news/illicit-uses-of-cryptocurrency-gaining-attention-around-the-world-expert-take.

[16] *See generally* Brito, *supra* note 1, at 10-11 (discussing the factors that make Bitcoin pseudonymous, not anonymous).

his or her public key a computer hard drive, analysts can find it and use it to uncover the suspect's entire transaction history. Also, it is possible that friends and associates may know a suspect's public key because they have sent virtual currency in the past. In these cases, law enforcement agencies may discover the key as a natural consequence of their regular investigation.

In many ways, Bitcoin and similar blockchain currencies can be helpful to law enforcement agencies. For example, the highly publicized arrest and conviction of Ross Ulbricht, founder of the online black marketplace "the Silk Road" shuttered by the FBI in 2013, was partially based upon the government's ability to trace Bitcoins sent from Silk Road to Ulbricht's personal wallets.[17] In an unanticipated twist also facilitated by the blockchain ledger, the government arrested two federal agents who had worked on the Silk Road case. Allegedly, they stole huge sums of money in virtual currency under the erroneous belief they could never be found out.[18]

Because it is a new way to exchange currencies, regulators have expressed concern about blockchain currencies' potential as an avenue for money laundering. However, virtual currency exchanges have a history of cooperating with anti-money-laundering policies, and the high degree of transparency in the public ledger system makes these currencies less attractive as a means of money laundering than traditional cash. In fact, laundering money through blockchain currencies can be much riskier than other systems. Once an investigator links a money launderer's Bitcoin address to his or her identity, law enforcement authorities have a complete record of all transactions.[19] As discussed below, increased regulation of virtual currency markets will likely accelerate the implementation of money laundering prevention policies within blockchain currency exchanges.

Regulators have expressed concern over the lack of a central authority that controls the decentralized blockchain currencies. Without central management, activities like due diligence, regulatory compliance, and monitoring and reporting of illegal activity may be more challenging. The FBI has expressed concern that decentralized blockchain currencies lack anti-money laundering software and do not require identifying information for account owners, in addition to the concern about the inability to completely shut-down a currency exchanging operating on a peer-to-peer network. [20] Additionally, there are several ways that virtual currency users can increase

[17] *Id.* at 11-12.

[18] *Id.* at 12 (indicating that the agents were discovered after blockchain analysis traced to public keys linked to the agent's identities).

[19] *See id.* at 1; *But see* FBI Directorate of Intelligence, BITCOIN VIRTUAL CURRENCY: UNIQUE FEATURES PRESENT DISTINCT CHALLENGES FOR DETERRING ILLICIT ACTIVITY 1 (2012) [hereinafter FBI Directorate of Intelligence] (indicating that an FBI investigation found "with low confidence" that Bitcoin will be used increasingly to launder money, but that this confidence level was limited due to limited data available at that time).

[20] *See* FBI Directorate of Intelligence, *supra* note 18, at 4-5 ("Since Bitcoin does not have a centralized authority, detecting suspicious activity, identifying users, and obtaining transaction records is problematic for law enforcement.").

their anonymity. Black Market websites like the Silk Road, for example, combine the virtual currency blockchain protocol with Tor networking to make illicit online transactions virtually untraceable.[21] As a result, it is likely that Bitcoin and similar products will continue to be used for the purchase of illicit goods online.[22]

Blockchain currency use in the black markets of the Dark Web has harmed this new technology's reputation. While the Silk Road was only responsible for a tiny fraction of total Bitcoin transactions, it has built a permanent association between blockchain currency and illicit online activity. Indeed, blockchain currencies can be specifically designed for illicit online use by making the transaction record opaque.[23] Nonetheless, the clear majority of blockchain currencies require individuals to make exchanges that are recorded on the public blockchain, which may provide the centralized authority law enforcement agencies with the information necessary to track and report illegal transactions.[24]

C. Theft and Fraud

The increasing value of blockchain currencies like Bitcoin and Ethereum also make virtual currency users targets for cybercriminals. While hackers have never successfully penetrated the blockchain underlying Bitcoin, virtual currency accounts known as "wallets," can be hacked by the same means hackers access a person's traditional bank account. Poor password management by account holders and inadequate security management within virtual currency exchanges are some of the greatest threats to virtual currency account security. Most wallets can be encrypted, which is an important

[21] *See* Brito, *supra* note 1, at 38-39 (discussing how The Silk Road was shuttered by the FBI in 2013, but as of 2016, approximately 30 known Deep Web black markets were operable).

[22] *See* FBI Directorate of Intelligence, *supra* note 18, at 1 (providing that the FBI found with "medium confidence that, in the near term, cyber criminals will treat Bitcoin as another payment option alongside more traditional and established virtual currencies…[and] with high confidence…that criminals intending to steal bitcoins can target and exploit bitcoin services and an individual's Bitcoin wallet…[and that] Bitcoin will likely continue to attract cyber criminals who view it as a means to move or steal funds as well as a means of making donations to illicit groups…"); *see also* Brito, *supra* note 20, at 38 (providing that developers have "started experimenting with distributed Deep Web market platforms that theoretically cannot be shut down by targeting any one server or operator.").

[23] *See* Andy Greenberg, *Monero, The Drug Dealer's Cryptocurrency of Choice, Is on Fire*, WIRED (Jan. 25, 2017)), https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/ (discussing a virtual currency known as Monero which operates on a protocol designed to be completely anonymous and untraceable and is increasing in popularity in the black markets on the Deep Web. Monero increased in value by over 2,700% in 2016 alone, outperforming all other competitors); *see also* Brito, *supra* note 20, at 24 (providing that another virtual currency, Zcash, is developing a protocol that has even greater privacy protections and liquid fungibility than Bitcoin).

[24] FBI Directorate of Intelligence, *supra* note 18, at 7 (providing that a centralized tracking system may allow authorities to track and report illegal transactions).

deterrent to cybertheft via malware. Despite these protections, virtual currency exchanges have experienced major hacks over the past few years.

Cryptocurrency holders keep encrypted wallets that can either be hosted by an online wallet service or downloaded onto a device. These wallets hold the private keys needed to access virtual funds. Without a private key, wallet owners cannot retrieve their virtual money. Because miners must verify every transaction by a majority consensus, it would require deceiving more than 50% of the entire network just to make one fraudulent conveyance. This degree of collusion is theoretically possible, but it is highly unlikely. So, a hacker can only perpetrate a theft in this manner if he or she controls more than half of the entire Bitcoin network's computational power.[25] Instead, when Bitcoin wallets are hacked, cybercriminals typically find passwords through more conventional methods like phishing and cracking.[26]

Bitcoin's security record is strong, but it is not impeccable. Unfortunately, cryptocurrency exchanges have been subject to hacks that created millions of dollars in financial liabilities. For example, between 2012 and 2015, several millions of dollars' worth of Bitcoin cybercurrency was stolen by hackers who were able to breach secure Bitcoin exchanges. Mt. Gox, the first functional blockchain currency exchange, controlled around 70% of all Bitcoin transactions in 2013. The following year, Mt. Gox filed for bankruptcy, apparently due to the theft of an astounding 850,000 Bitcoins: equivalent to $473 million at the time. Because blockchain currency wallets are not federally-insured, like securities accounts or bank accounts at licensed financial institutions, Mt. Gox left many customers with no recourse for their loss. Fortunately, Mt. Gox has served as a cautionary tale in Bitcoin markets, with most new Bitcoin companies taking proactive measures to ensure the integrity of their trading systems and protect their customers from fraud. [27]

Cryptocurrency exchanges that are not regulated lack many of the investor protections required by law in other markets. As hackers become more sophisticated, this will create growing risk in virtual commodity markets. According to global thinktank Ernst & Young, over 10%of funds going towards new coins created by Initial Coin Offerings ("ICOs") are lost or stolen. Hackers have cost the cryptocurrency market nearly $400 million in new coins stolen from otherwise legitimate ICOs, further exacerbating the

[25] *See generally* Jameson Lopp, *Bitcoin's Security Model: A Deep Dive*, COINDESK (Nov. 13, 2016) https://www.coindesk.com/bitcoins-security-model-deep-dive/.

[26] *See How to Store Your Bitcoins*, COINDESK, https://www.coindesk.com/information/how-to-store-your-bitcoins/ [last updated (Oct. 19, 2015)] (discussing how there are several things that cryptocurrency holders can do to increase the security of their wallets. For example, a wallet can be downloaded to a separate hard drive that is not connected to the internet. Online wallets can also be protected using multi-signature transactions.).

[27] *See* Brito, *supra* note 1, at 35-36 (highlighting companies like Coinbase and BitGo who prominently publicize their account security insurance policies to customers and Bitcoin exchanges like Kraken that undergo third-party audits to ensure their ability to cover customer balances).

risk of investing in these ventures.[28] What is worse, theft has been increasing within cryptocurrency markets as hackers become more and more sophisticated.

To date, cybercriminals have stolen an estimated $4 billion from cryptocurrency exchanges and wallets so far, and almost none of these funds have been recovered.[29] As staggering as it is, this figure does not even include the dozens of hacks that have penetrated cryptocurrency exchanges since 2011. Thefts of cryptocurrency exchanges have caused the loss of an additional 980,000 Bitcoins across the market. Some have been recovered, but most have not been.[30] Some exchanges have responsibly responded to security breaches by repaying customers the value of stolen funds and subsequently beefing up security protocols.[31] Hopefully, however, as federal regulators increase law enforcement efforts, the pervasive financial crimes taking place within the cryptocurrency markets will subside.

Because blockchain currency exchange companies and creative Bitcoin entrepreneurs have been able to operate largely without regulatory oversight, there have been several instances of fraud and swindles in Bitcoin-based financial markets.[32] The SEC and other agencies have announced that they are focusing on developing ongoing efforts and launching new initiatives to combat fraud and related misconduct in blockchain currency markets.[33] However, agencies are still cracking down on existing blockchain currency-based Ponzi schemes designed to defraud investors.[34]

IV. REGULATION OF BLOCKCHAIN CURRENCIES

[28] Ernst & Young, Inc., *EY Research: Initial Coin Offerings*, (Dec. 31, 2017) http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf.

[29] Caleb Blair, Joseph Wall, Lewis Kilbourne, and Larry Crumbley, *Cryptocurrencies Are Taxable and Not Free from Fraud,* at 4, TAX NOTES TODAY (Jan. 23, 2018).

[30] *Cryptocurrency Exchanges Are Increasingly Roiled by Hackings and Chaos*, FORTUNE (Sept. 29, 2017) http://fortune.com/2017/09/29/cryptocurrency-exchanges-hackings-chaos/.

[31] Leo Lewis, *Hedge funds gamble on Mt. Gox bitcoin payout*, FIN. TIMES (Feb. 17, 2017) https://www.ft.com/content/821ae69a-f0d1-11e6-8758-6876151821a6 (explaining that Mt. Gox's approximately 24,000 aggrieved account holders are expected to be paid out about a quarter of the bitcoins and cash lost from their accounts).

[32] *See* Brito, *supra* note 1, at 22-23.

[33] Testimony of CFTC Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition and Forestry, at 12-13 http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6. (Dec. 10, 2014).

[34] Compl. at 1-2, Sec. & Exch. Comm'n v. REcoin Grp. Found. LLC et al., No. 17-cv-5725, *complaint filed*, 2017 WL 4329876, (E.D.N.Y. Sept. 29, 2017) (showing the SEC filed an emergency action to prevent Maksim Zaslavskiy and his two companies, REcoin Group Foundation, LLC and Diamond Reserve Club, from engaging in ongoing illegal and fraudulent offerings of new blockchain currencies. At the time of the complaint, the defendant had allegedly defrauded investors at least $300,000 over a span of only three months).

Cryptocurrencies raise novel issues for financial regulators, and federal agencies have struggled to develop a unified approach. Although virtual currencies can function as payment systems for goods and services, they do not fall within the legal definition of money.[35] They are not currency, but the federal courts have treated bitcoins and its progeny as money for certain purposes.[36] But, if cryptocurrencies are not money, what are they?

As with most questions, the response depends on whom you ask. The SEC defines cryptocurrencies as securities and demands all coin issuers and exchanges comply with the Securities Act of 1933 and the Securities and Exchange Act of 1934.[37] The CFTC, on the other hand, has treated virtual currencies as "commodities" subject to the Commodity Exchange Act since at least 2014.[38] The Internal Revenue Service ("IRS") characterizes virtual currencies as property subject to the capital gains tax rules,[39] whereas the Department of Treasury is more inclined to treat them as money under certain circumstances, much like the federal courts.[40]

This divergence in opinion makes for a challenging regulatory environment. The Treasury Department has taken a more active role in corralling financial regulators into a unified regulatory approach. Under the direction of Treasury Secretary Steve Mnuchin, the SEC, CFTC, and Financial Crimes Enforcement Network ("FinCEN"), and the Federal Reserve have established a working group to investigate cryptocurrency activities and develop an effective regulatory response. [41] However, this working group is in its infancy. As a result, a unified regulatory approach to cryptocurrency markets is still far off.

Although federal regulators have yet to develop a unified policy regarding cryptocurrency, investors should not expect business-as-usual. U.S. federal law enforcement agencies have ramped up enforcement efforts against illegal cryptocurrency activity, indicating that the market is under

[35] *See* Hepburn v. Griswold, 75 U.S. 603 (1869) (defining "money and legal tender" by nature of its relationship to a centralized government authority).

[36] *See* United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017) (explaining that although not traditional currency, Bitcoins and similar forms cybercurrency are considered money for certain purposes).

[37] United States Security and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities and Exchange Act of 1934: The DAO*, Release No. 81207 (July 25, 2017).

[38] *See* Testimony of CFTC Chairman Timothy Massad, *supra* note 32 at 12-13.

[39] INTERNAL REVENUE SERV., Notice 2014-21, at 1-2.

[40] U.S. Department of Treasury, Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, Guidance FIN-2013-G001, at 2.

[41] U.S. COMMODITY FUTURES TRADING COMM'N, *Testimony of CFTC Chairman J. Christopher Giancarlo before the U.S. Senate Committee on Banking, Housing and Urban Affairs* https://www.banking.senate.gov/public/index.cfm/2018/2/virtual-currencies-the-oversight-role-of-the-u-s-securities-and-exchange-commission-and-the-u-s-commodity-futures-trading-commission (Feb. 6, 2018).

more scrutiny than ever.[42] Regulators are responding more actively than they have in the past to indications of illegal activity in cryptocurrency markets. As a result, enforcement actions against market players engaging in price manipulation, unregistered securities trading, money laundering, and tax evasion are now much more likely to catch the attention of federal law enforcement officials than in the past.[43]

Since Bitcoin launched in 2009, cryptocurrency entrepreneurs have launched virtual currency derivative exchanges, stock markets, and other financial arrangements. However, most are operating outside the regulatory process. Several companies offering markets for the purchase and sale of Bitcoin derivatives have emerged, all denominated by Bitcoin currency. Other companies offer exchanges of shares of stock in Bitcoins, and a few burgeoning entrepreneurs have offered shares of stock in their own companies on these Bitcoin exchanges. The following summary provides a brief overview of the regulatory system currently affecting blockchain currencies, including a description of the types of activities regulated by several federal administrative agencies with jurisdiction.[44]

A. Blockchain Securities and "Initial Coin Offerings"

Once Bitcoin launched, the intellectual property that went into developing blockchain currency became public. It was only a matter of time until programmers replicated this technology and used it for new purposes. There are now approximately 1,163 distinct types of blockchain currencies in the virtual currency market.[45] Over time, the SEC has exerted its jurisdiction over the distribution of new blockchain currencies through ICOs, an increasingly common method of raising capital.

[42] Robert J. Anello and Christina Lee, *New-Wave Legal Challenges for Bitcoin and Other Cryptocurrencies*(2017) https://www.law.com/sites/almstaff/2017/11/07/new-wave-legal-challenges-for-bitcoin-and-other-cryptocurrencies/?slreturn=20180315172853 (describing law enforcement's increased scrutiny of Bitcoin and other cryptocurrencies to ensure more regulation).

[43] *See* Ernst & Young, Inc., *supra* note 27 at 36.

[44] *See generally* Peter Van Valkenburgh, *Tracking Bitcoin Regulation State by State*, COINCENTER (June 2, 2015) https://coincenter.org/entry/tracking-bitcoin-regulation-state-by-state (passing cryptocurrency regulations by states that apply to virtual transactions in their jurisdiction. Hawaii, for example, regulates digital currency exchanges as money transmitters and requires all exchanges to hold cash reserves equal to the amount of virtual currency held by all customers. New York recently passed laws creating a licensing system for digital currency, while states like New Hampshire and Connecticut have left the regulatory agencies with the sole discretion to regulate cryptocurrencies).

[45] COINMARKETCAP, *Current Market Capitalizations* (Oct. 13, 2017) https://coinmarketcap.com/all/views/all/ (finding that some virtual currencies are simply Bitcoin duplicates, but others seek to improve on the model. For example, the popular altcoin known as Litecoin mimics Bitcoin's system but uses a modified algorithm in which coin mining and verification have lower hardware requirements); *see* Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* 1 (2016) https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv2_0.pdf. .

In 2014, the SEC prosecuted Erik Voorhees, the owner of two Bitcoin-based e-commerce websites that sold equity shares in his companies for blockchain currency. Since he did so without first receiving approval from the SEC, the defendant business owner violated Sections 5(a) and 5(c) of the Securities Act and settled with the agency.[46] Two years later, the agency brought a similar case against Bitcoin Investment Trust and SecondMarket Inc. on the basis that the companies were selling shares of equity in exchange for Bitcoin. These companies also settled the action with an agreement to cease all prohibited activity and pay a disgorgement fee.[47] Despite these early cases demonstrating the SEC's position on Initial Coin Offerings, the agency continues to prosecute individuals for the unregistered offer and sale of securities denominated in blockchain currencies.[48]

On July 25, 2017, the SEC issued a report clarifying the agency's position that virtual blockchain currencies are securities that fall under the jurisdiction of the Securities Act of 1933 and the Securities and Exchange Act of 1934. In this report, the agency clarified that "virtual organizations or capital raising entities that use distributed ledger or blockchain technology to facilitate capital raising and/or investment and the related offer and sale of securities," must comply with federal securities laws.[49] The SEC noted that blockchain technology was being used increasingly as an instrument to raise capital for new businesses in sales that have become known as ICOs and under certain facts and circumstances, these sales must comply with U.S. securities law.[50]

To comply with Section 5 of the Securities Act, ICOs must register with the SEC before any entity can offer to sell or buy the new virtual currency. The agency came to this conclusion based on the precedent set forth by the U.S. Supreme Court in *SEC v. W.J. Howey Co*, 328 U.S. 293 (1946). In this case, the Court developed a standard to determine whether a particular financial instrument qualifies as an "investment contract" under the Securities Act. Specifically, the *Howey* test requires regulators to determine whether a financial offering "involves an investment of money in a common

[46] In the Matter of Erik T. Voorhees, Order Instituting Cease-And-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, Making Findings, and Imposing a Cease-And-Desist Order, Admin. Pro. File No. 3-15902, Release No. 9592 (June 3, 2014) at https://www.sec.gov/litigation/admin/2014/33-9592.pdf..

[47] In re Bitcoin Investment Trust and SecondMarket, Inc., Order Instituting Cease-And-Desist Proceedings Pursuant to Section 21C of the Securities Act of 1934, Making Findings, and Imposing a Cease-And-Desist Order, Admin. Pro. File No. 3-17335, Release No. 78282 (July 11, 2016) https://www.sec.gov/litigation/admin/2016/34-78282.pdf.

[48] *See generally Report of Investigation Pursuant to Section 21(a) of the Securities and Exchange Act of 1934: The DAO*, Release No. 81207 SEC (July 25, 2017) https://www.sec.gov/litigation/investreport/34-81207.pdf.

[49] *Id.* at 2.

[50] *Id.* at 10.

enterprise with profits to come solely from the efforts of others," regardless of the corporate form or type of security the organization has offered.[51]

In other words, companies soliciting investments of money – either fiat currency or virtual – for a common enterprise from investors who have a reasonable expectation of return based on the managerial efforts of others must first register with the SEC or face prosecution for federal securities violations.[52] For companies currently operating blockchain currencies without SEC licensing, regulatory compliance should be an immediate priority.

The SEC started prosecuting companies for issuing equity-based and commodity-backed securities without first securing regulatory approval in 2014. In that year, the SEC prosecuted Ethan Burnside and his company, BTC Trading, for buying, selling, and trading blockchain currencies issued on his website as ICOs. The exchange accepted only Bitcoin and another popular virtual currency, Litecoin, while advertising to users that they could "experiment with virtual currency investing by purchasing stock in virtual currency," or "start a virtual currency company and issue stock to raise funds" for the business.[53] However, BTC Trading's exchanges occurred without first registering with the SEC pursuant to the Securities Act and Securities and Exchange Act. Thus, the defendant was forced to repay profits gained from the websites, in addition to refunding fees and a 2-year suspension from any regulated securities-related activity.[54]

Section 5 of the Securities and Exchange Act prohibits the exchange of securities unless the SEC registers the activity as a national securities exchange.[55] An "exchange" is "any organization, association, or group of persons, whether incorporated or unincorporated, which constitutes, maintains, or provides a market place or facilities for bringing together purchasers and sellers of securities."[56] This broad definition for exchange can apply to any activities that mimic a stock exchange, regardless of the business form, venue, or currency accepted.

While most blockchain currency-based securities exchanges have avoided regulation in what was formerly a legal gray area, it is now clear that SEC policy requires registration for all non-exempt securities and transactions.[57] The SEC recently specified that any online program matching

[51] SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946).

[52] *See* Report of Investigation, *supra* note 47.

[53] In re BTC Trading, Corp. and Ethan Burnside, Order Instituting Administrative and Cease-And-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, Sections 15(b) and 21c of the Securities Exchange Act of 1934, and Section 9(b) of the Investment Company Act of 1940 Making Findings, and Imposing a Cease-And-Desist Order, Admin. Pro. File No. 3-16307, Release No. 9685, at 3 (Dec. 8, 2014).

[54] *Id.* at 10-11.

[55] 15 U.S.C. § 78e (2017).

[56] 15 U.S.C. § 78c(a)(1) (2017).

[57] S.E.C. Act, § 201 (2005) (listing nine types of exempt securities: government securities, legitimate foreign securities, banks and depository institutions, insurance, railroads and utility securities, options or warrants, nonprofits, employee benefit plans, and employment

securities orders from various parties seeking to buy and sell blockchain securities qualify as a security exchange requiring regulatory review and approval. Ultimately, the determination of whether a specific blockchain currency falls under SEC jurisdiction depends on the facts and circumstances of the individual case.[58] The SEC has also started to focus its enforcement authority on cryptocurrency markets.

In January of 2018, SEC Chairman Jay Clayton and CFTC Chairman J. Christopher Giancarlo expressed concern about the lack of transparency and investor protection in cryptocurrency markets. The agencies see cryptocurrency markets as "show[ing] little or no regard to our proven regulatory approach."[59] As a result, they are ramping up enforcement efforts, especially with unregistered ICOs.

Between December 2017 and January 2018, the SEC initiated several significant actions against ICO issuers and cryptocurrency exchanges through its new Cyber Unit. Although the agency just created the Cyber Unit in September 2017, the Cyber Unit has already sent a message to cryptocurrency companies that it means business. It filed its first enforcement action on December 1, 2017 against PlexCorps and its founders based on an ICO for "PlexCoins" that were released in August 2017. On December 4, the Commission obtained an emergency asset freeze against PlexCorps and charged its founders, Dominic Lacroix and Sabrina Paradis-Roger, for allegedly raising over $15 million from a fraudulent and unregistered ICO. Lacroix and Paradis-Roger have been charged under the anti-fraud and registration provisions of the Securities Act and Exchange Act, and are facing substantial fines and penalties.[60]

Just one week after the PlexCorps order, the SEC settled another ICO enforcement action against Munchee, Inc. Munchee voluntarily ceased its ICO, but the SEC emphasized that any token sale giving investors a reasonable belief that their coin purchase would generate a return gave rise to possible liability under securities laws.[61]

trust certificates. The USA also exempts several types of non-issuer transactions, transactions in foreign-issued securities, and securities exchanges where no cash is involved in any transaction. Most commonly, cryptocurrency exchanges claim exemption under the exclusion of non-cash transactions).

[58] *See Report of Investigation Pursuant to Section 21(a) of the Securities and Exchange Act of 1934: The DAO*, Release No. 81207 SEC (July 25, 2017) https://www.sec.gov/litigation/investreport/34-81207.pdf..

[59] Jay Clayton & J. Christopher Giancarlo, *Regulators Are Looking at Cryptocurrency*, WALL STREET JOURNAL (Jan. 24, 2018) https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363.

[60] SEC v. PlexCorps, No. 17 Civ. 7007 (CBA), 2017 WL 6398722 at * 1 (E.D.N.Y. Dec. 14, 2017).

[61] In the Matter of Munchee, Inc., Order Instituting Cease-and-Desist Procedings Pursuant to Section 8A of the Securities Act of 1933, Making Findings, and Imposing a Cease-and-Desist Order, Admin. Pro. 3-18304, Release No. 10445, (Dec. 11, 2017) https://www.sec.gov/litigation/admin/2017/33-10445.pdf.

The PlexCorps and Munchee actions were meant to be a shot across the bow for new ICOs. The SEC continues to prosecute unregistered ICOs, starting with ones that raise the greatest suspicion of fraudulent activity. On January 25, 2018, the SEC filed suit against AriseBank and its founders, Jared Rice Sr. and Stanley Ford, for launching an allegedly fraudulent ICO for "AriseCoin." A federal court halted the coin sale on January 30, and the SEC seeks disgorgement of all proceeds plus the payment of interests and penalties.[62]

Given the escalation of SEC enforcement activity since the agency concluded its extensive investigation of the DAO in July 2017, cryptocurrency exchanges and ICO issuers can expect greater scrutiny from securities regulators. However, the SEC is dealing with substantial limitations to its jurisdictional authority. The agency initiated the aforementioned enforcement cases against companies and individuals located in the United States. The Supreme Court established how regulators enforce domestic securities laws outside of the territorial United States in *Morrison v. National Australia Bank*, 561 U.S. 247 (2010). In this case, the Court held that U.S. securities laws only apply outside the U.S. when there is a clear indication in the statutory language that Congress intended extraterritorial jurisdiction. Because the Exchange Act has no clear language in this regard, the Court decided that federal agencies can pursue securities fraud charges only against companies listed on U.S. exchanges or transacting securities in the United States. As a result, under the Morrison standard, it is unlikely that the SEC can take any enforcement action against ICOs launched outside the United States, despite the fact that they disregard for domestic laws.

However, it is possible that the rule set forth in *Morrison* could change if the SEC chooses to pursue extraterritorial enforcement by the Dodd-Frank Act, passed just weeks after the Supreme Court decided *Morrison*.[63] Under Dodd-Frank, U.S. courts have jurisdiction over securities violations that occur in the United States even if the company or transactions at issue are outside the country.[64] The question of whether regulators can use this provision of the Dodd-Frank Act as a basis for extraterritorial enforcement of U.S. securities laws is an untested question. If doing so will help curb domestic violations of securities laws, the SEC may well decide to pursue foreign ICOs due to their impact on financial stability in the U.S.

The question of how the Dodd-Frank Act impacts the scope of SEC authority under *Morrison* is critical to determining securities liability for ICOs and other international cryptocurrency transactions. *Morrison* limited securities enforcement to territorial U.S. jurisdictions, absent express authorization from Congress to the contrary. In the digital currency world, however, it is exceedingly simple to avoid this limited jurisdiction. Because

[62] SEC v. AriseBank, Dkt. No. 3:18-cv-00186 (N.D. Tex. Jan. 25, 2018).

[63] Dodd-Frank Wall Street Reform and Consumer Protection Act, 15 U.S.C. § 780 et seq. (2010).

[64] 12 U.S.C. § 5331 (2010).

they are entirely online, most cryptocurrency users can easily remove their transactions from U.S. territorial jurisdiction. Even ICOs who do end up facing securities enforcement actions can only be held liable for violations that took place in the United States. Under this standard, SEC enforcement does not have much of a bite to it. However, if the law shifts to a more expansive view of SEC enforcement jurisdiction under Dodd-Frank, this all may change. Under Dodd-Frank, the SEC could exert jurisdiction over coin sales outside the United States if wrongful activity has a substantial foreseeable effect on U.S. markets. This expansion of SEC jurisdiction could substantially expand the agency's enforcement authority and suppress ICO activity across the board.[65]

B. Blockchain Currency Futures and Derivatives

The SEC is not the only agency that has attempted to reign in unregulated financial activities in blockchain currency markets by regulating blockchain currencies as *securities* rather than traditional money. The Commodity Futures Trading Commission ("CFTC") regulates commodity futures, which has a limited application in a market where a coin is exchanged instantaneously through a peer-to-peer network. Instantaneous exchanges are not futures contracts, and therefore the CFTC is limited in their authority to regulate. However, in the instances where the CFTC exerts its jurisdiction, it has engaged in rigorous enforcement and regulated blockchain currencies with a measured hand, taking a "do not harm" approach to the technology to maintain the innovative benefits of this new technology.[66]

The Commodity Exchange Act of 1936 defines commodities as "goods and articles... and all services, rights, and interests... in which contracts for future delivery are presently or in the future dealt in."[67] Investors can trade Bitcoin and other blockchain currencies through futures contracts, and therefore these assets fall squarely within the legal definition of a commodity and the jurisdiction of the CFTC. In its first action against an unregulated blockchain currency options trading platform, the CFTC instituted proceedings against Francisco Riordan and his company Coinflip, Inc. based upon the defendant's offering of Bitcoin options and futures contracts in 2015. The agency found that the defendant violated Sections 4c(b) and 5h(a)(1) of the Commodity Exchange Act, as well as implementing Commission Regulations 32.2 and 37.3, and he was ordered to cease all prohibited activity.[68]

Unlike the SEC, which has yet to license any platform for the exchange of virtual currency-based securities, the CFTC has been issuing provisional

[65] *See* Anello, *supra* note 41 at 1, 4.

[66] *See generally* Brito, supra note 1 at 57-58.

[67] 7 U.S.C. § 1a(9) (2017).

[68] In the Matter of Coinflip, Inc., CFTC No. 15-29 (Sept. 17, 2015).

registrations to blockchain currency swap markets since 2014.[69] The CFTC's openness to integrating this new technology into the options markets it regulates can prove beneficial for the future of blockchain currencies, as it may help mitigate the cryptocurrency market's famous price volatility. Virtual currency derivatives markets can have a stabilizing effect on the price of traded blockchain currencies, and effective regulation of these markets can have a positive impact on the development of these new commodities.[70]

Unlike the SEC, the CFTC has been more receptive to cryptocurrency and has been more forthcoming with derivatives approvals. Whereas the SEC has not approved any bitcoin derivatives,[71] the CFTC approved bitcoin futures products and bitcoin binary options in December 2017.[72] The CFTC's progress in this regard may give virtual currency investors the impression that the agency is more flexible with respect to enforcement actions dealing with virtual currency. However, nothing could be further from the truth.

On January 16, 2018, the CFTC charged My Big Coin Pay, Inc. and its founders Randall Crater and Mark Gillespie with fraud and misappropriation of investor's funds. The complaint alleges that the defendants took over $6 million from My Big Coin Pay customers and transferred it to their private bank accounts for personal use.[73] Commenting on the case, CFTC Director of Enforcement James McDonald explained, "As this case shows, the CFTC is actively policing the virtual currency markets and will vigorously enforce the anti-fraud provisions of the Commodity Exchange Act."[74]

[69] TeraExchange, LLC received provisional registration from the CFTC as a Bitcoin swap execution facility in 2013; *see* In the Matter of TeraExchange LLC, CFTC No. 15-33 (Sept. 24, 2015) (LedgerX, LLC has been fully-approved as a Bitcoin derivatives clearing organization and swap execution facility as of July 2017; *see* CFTC Order of Registration, In the Matter of the Application of LedgerX, LLC For Registration as a Derivatives Clearing Organization (July 24, 2017). http://www.cftc.gov/idc/groups/public/@otherif/documents/ifdocs/ledgerxdcoregorder72417.pdf; *see* CFTC Order of Registration, In the Matter of the Application of LedgerX LLC for Registration as a Swap Execution Facility (July 6, 2017), http://www.cftc.gov/idc/groups/public/@otherif/documents/ifdocs/orgledgerxord170706.pdf.

[70] *See supra* note 66, at 31-32.

[71] *See* Order Disapproving a Proposed Rule Change, Exchange Act Release No. 34-80319, 82 Fed. Reg. 16247 (April 3, 2017) (disapproving listing and trading of shares of SolidX Bitcoin Trust as Commodity-Based Trust Shares on the NYSE); Order Disapproving a Proposed Rule Change, Exchange Act Release No. 34-80206. 82 Fed. Reg. 14076 (March 101610, 2017) (disapproving Batz BTX Exchange's application to list and trade Commodity Based Trust Shares issued by the Winklevoss Bitcoin Trust).

[72] U.S. COMMODITY FUTURES TRADING COMM'N,, *CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE, and Cantor Exchange,* Press Release No. pr7654-17 (Dec. 1, 2017).

[73] Commodity Futures Trading Comm'n v. My Big Coin Pay, Inc. et al., CFTC. No. 1:18-cv-10077-RWZ (Jan. 16, 2018); *see* In the Matter of TeraExchange LLC, CFTC No. 15-33 (Sept. 24, 2015).

[74] U.S. COMMODITY FUTURES TRADING COMM'N,, *Federal court issues restraining Order freezing Defendants' and Relief Defendants' assets and protecting books and records*, Press Release No. pr7678-18 (Jan. 24, 2018).

Already, it is clear that Director McDonald was not bluffing. Just two weeks after the CFTC filed the My Big Coin case, media reports surfaced regarding the agency's investigation of Bitfinex, a popular cryptocurrency exchange, and Tether, a cryptocurrency designed to mirror U.S. dollar value. While the investigation has been kept relatively quiet, the agency is concerned that the exchange is manipulating the price of Tether and fraudulently claiming that it holds $2.3 billion in U.S. dollars to back the currency's value.[75] If the rumors are true, this would be the second enforcement action the CFTC has taken against the exchange.[76]

According to a report issued by the CFTC's Office of Public Affairs on January 8, 2018, the agency intends to continue to assert legal authority over virtual currency derivatives suspected of fraud or price manipulation. The CFTC also plans "robust enforcement" of laws addressing fraud, abuse, manipulation, or false solicitation in cash or spot markets trading in virtual currencies. Additionally, the CFTC engages in "heightened review" of virtual currency derivatives clearing markets, ensuring that the agency has greater authority to monitor and police these transactions.[77]

C. Federal Money Transmission and Money Laundering Regulation

Federal and state laws require businesses to license themselves as money transmitters if they transmit funds from one person to another. The U.S. Government lawfully prohibits the operating of an unlicensed money transmission company in 48 states and the District of Columbia, and they made it a federal offense under the USA PATRIOT Act in 2001.[78] Further, under a policy intended to deter money laundering and the financing of terrorism found in the Bank Secrecy Act of 1970, FinCEN has the authority to enforce financial crimes related to unauthorized money transmission.[79]

Financial institutions, including money transmitters, must register with FinCEN and implement specific anti-money laundering programs to comply with the Bank Secrecy Act, the Patriot Act, and implementing regulations. Users of convertible virtual currencies – those which can be exchanged for fiat money - are not all subject to FinCEN regulation. Rather the agency regulates all businesses that exchange virtual currency for real currency, virtual currency, or other funds ("exchangers") and all individuals engaged in the business of issuing and redeeming virtual currency into circulation

[75] Matthew Leising, U.S. Regulators Subpoena Crypto Exchange Bitfinex, Tether, *Bloomberg* (Jan. 30, 3018 8:26 PM) https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc.

[76] In the Matter of BXFNA Inc. d/b/a Bitfinex, CFTC No. 16-19 (June 2, 2016).

[77] U.S. COMMODITY FUTURES TRADING COMM'N,, *CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets* (Jan. 4, 2018) http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/backgrounder_virtualcurrency01.pdf.

[78] *See* Brito, *supra* note 1 at 43; *See also* 18 U.S.C. § 1960 (2001).

[79] 31 U.S.C. §§ 5311 et seq. (2001).

("administrators") as money services businesses ("MSBs"). An MSB must register with FinCEN and follow the agency's regulations regarding recordkeeping, reporting, and anti-money laundering measures.[80]

Since 2013, administrative courts have clarified exactly which actors in the blockchain currency economy qualify as exchangers and administrators. This subsequent guidance indicates that blockchain currency exchange markets (those which provide users with a marketplace through which virtual currencies can be exchanged) and payment processing companies (those which accept and transmit funds between merchants and consumers to achieve a sale of goods) are "exchangers" subject to FinCEN oversight and likely state licensing requirements in the future.[81] In 2015, FinCEN resolved an enforcement action against Ripple Labs Inc. and its corporate predecessors for operating as a currency exchange service without registering with regulators or making required disclosures. Specifically, Ripple Labs facilitated transfers of virtual currencies for fiat money or other virtual currencies and issued its virtual currency known as XRP, raising up to $1.3 million in capital in a single month.[82] The case was settled for fees and penalties, but Ripple Labs was allowed to continue operating so long as it complied with the Bank Secrecy Act and FinCEN regulations.[83]

Despite its broad authority to curb money laundering and terrorist financing, FinCEN has not yet ramped up its enforcement actions to the same degree as the SEC and CFTC have in late 2017 However, similarly aggressive law enforcement tactics may be on the horizon. In late 2017, FinCEN brought criminal charges against a defendant offering private bitcoin-for-cash exchanges through popular website LocalBitcoins.com. However, this case represents only the most recent of several cases the agency has brought against defendants charged with transmitting money without a license based on in-person bitcoin-for-cash transactions.[84] In December, a federal court sentenced one such defendant to one year and a day in jail for providing unlicensed money services in 2015. Specifically, he was found to have funneled $2.4 million worth of bitcoins through a corporation he owned. The Defendant, Sal Mansy, was also ordered to forfeit $118,000 in cash and bitcoin.[85]

[80] U.S. Dep't of Treasury FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, Guidance FIN-2013-G001, 2 (March 18, 2013).

[81] *See supra* note 77, at 44-45.

[82] United States v. Ripple Labs Inc., U.S. Dep't of Justice, (May 5, 2015), https://www.justice.gov/opa/pr/ripple-labs-inc-resolves-criminal-investigation.

[83] *Id.* at 12, 13.

[84] Nikhilesh De, *Michigan Man Charged for Unlawful Bitcoin Exchange*, COINDESK (Oct. 27, 2017) https://www.coindesk.com/michigan-man-charged-unlawful-bitcoin-exchange.

[85] Department of Justice, *Detroit Man Sentenced to a Year and a Day for Operating an Unlicensed Bitcoin Business* (Dec. 4, 2017) https://www.justice.gov/usao-me/pr/detroit-man-sentenced-year-and-day-operating-unlicensed-bitcoin-business.

FinCEN has been relatively consistent in virtual currency-based financial crimes enforcement, but like the SEC and CFTC, it will most likely accelerate enforcement efforts shortly. The SEC is limited in its ability to enforce securities laws against foreign actors in the cryptocurrency markets. However, the Department of Justice and FINCEN are not similarly limited. Rather, they have broad authority to reach financial criminals overseas.[86] As a result, it appears that anti-money-laundering regulations and laws regarding money transmitters may be more effective law enforcement mechanisms for curbing financial abuses in the cryptocurrency markets. The Treasury Department is currently reviewing FINCEN's virtual currency policies, and it is likely to shift how it identifies and prioritizes money laundering and terrorist financing risks created by cryptocurrencies.[87]

D. Taxation

The IRS issued a policy statement in 2014 clarifying the agency's position regarding the taxation of virtual currencies. In this statement, the IRS stated that even though individuals and businesses may use blockchain currencies to purchase and sell goods, they are also convertible into U.S. dollars or other fiat currencies. Partially based upon FinCEN's 2013 findings regarding the classification of virtual currencies as commodities rather than currency, the IRS concluded that blockchain currency proceeds must be taxed as property rather than currency or income.[88]

Like other property, the IRS taxes cryptocurrency proceeds at the capital gains tax rates. While this policy clarification is helpful in eliminating any uncertainty among blockchain currency users, it has created some complications for virtual currency holders. For example, if a user purchases a virtual currency when the market price is $30 per coin and then purchases an ice cream cone with some of this coin when the market price is $40, she owes capital gains taxes on the value of that expenditure. Indeed, the administrative complexity and enforcement resources necessary to ensure businesses and individuals pay taxes on every taxable blockchain currency transaction could be extraordinarily high.[89]

[86] In July 2017, the Department of Justice filed a criminal case against BTC-e – a major foreign cryptocurrency exchange – as well as its founder Alexander Vinnik, who is a Russian national. FINCEN also imposed a fine of $110 million against BTC-e and an additional $12 million against Vinnik personally for engaging in unlawful monetary transactions. *See* In the Matter of BTC-E, U.S. Department of Treasury Financial Crimes Enforcement Network, No. 2017-03 (July 26, 2017) https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf.

[87] Department of the Treasury, Annual Plan Fiscal Year 2018, 57 (October 2017) https://www.treasury.gov/about/organizational-structure/ig/Audit%20Reports%20and%20Testimonies/OIG-CA-18-005.pdf.

[88] INTERNAL REVENUE SERV., Notice 2014-21, 2.

[89] *See* Brito, *supra* at 55-56.

The IRS has been very clear regarding the taxation of virtual currencies as property.[90] Although this policy has been firmly in place since 2014, the IRS has evidence of substantial under-reporting of cryptocurrency income. In fact, the agency received only 802 tax returns reporting cryptocurrency gains in 2015 despite the fact that domestic cryptocurrency exchanges processed millions of transactions between 2013 and 2015.[91] However, due to the anonymous and decentralized nature of virtual currencies, the IRS faces substantial obstacles to bringing cryptocurrency tax evaders to justice.

In a bold enforcement move, the IRS has decided to work around the anonymity issue by forcing cryptocurrency exchanges to reveal identifying information about suspected tax evaders. In *United States v. Coinbase Inc.*,[92] the IRS sought taxpayer information from Coinbase, America's most popular Bitcoin exchange. Just after Thanksgiving last year, a federal court in the Northern District of California ordered Coinbase, the largest Bitcoin exchange in the United States, to provide the IRS with identifying information on over 14,000 of its users. Specifically, Coinbase must disclose the name, date of birth, address, and taxpayer ID of these customers, most of whom were the highest-volume traders between 2013 and 2015.[93] While it remains to be seen what the IRS will do with this information, it is safe to assume that it will identify and prosecute some tax evaders in the very near future.

E. Consumer Protection

As discussed previously, the innovative character of blockchain currencies has created an avenue for duplicitous individuals to commit fraud. Because there is no federal insurance on deposits into blockchain currency wallets, consumers who have been the victim of fraud often find themselves with little recourse. The Consumer Financial Protection Bureau ("CFPB") has started accepting complaints from consumers who experience loss through fees, hacking, fraud, or other schemes associated with blockchain currency holdings.[94]

The CFPB may have the authority to regulate virtual currency under the Electronic Fund Transfer Act, which defines an electronic transfer as "any transfer of funds," not "originated by check, draft, or similar paper instrument," and "which is initiated through an electronic terminal."[95]

[90] INTERNAL REVENUE SERV., Notice 2014-21, 3.

[91] *See* Blair, *supra* note 28, at 2.

[92] United States v. Coinbase Inc., et al., No. 3:17-cv-01431, 2017 WL 5890052 (N.D. Cal. Nov. 28, 2017).

[93] *Id.*

[94] Consumer Financial Protection Bureau, *What are virtual currencies and what should I know if I'm interested in using one?*, Ask CFB (April 15, 2016) https://www.consumerfinance.gov/ask-cfpb/what-are-virtual-currencies-and-what-should-i-know-if-im-interested-in-using-one-en-1893/.

[95] 15 U.S.C. § 1693a(7) (2017).

However, the definition also specifically excludes "the purchase or sale of securities through a broker-dealer registered with or regulated by the SEC."[96] Because the SEC has exerted jurisdiction over blockchain currency exchanges, the CFPB's place in the regulatory mix remains unclear. Other than accepting complaints and issuing consumer advisories on the risk of fraud associated with blockchain currency investments, the CFPB has not issued any statements regarding the agency's policy toward virtual currency consumer protection.[97]

V. STATE LAWS REGARDING CRYPTOCURRENCY

Like the federal financial regulators, most states are still in the early stages of investigating what policies they should develop and enforce against cryptocurrency investors and exchanges. However, the federalist system has long relied on states as laboratories for public policy, and some have already developed progressive new laws regarding cryptocurrencies.

State money transmission regulations regarding blockchain currency transfers have been a bit slower to develop than FINCEN policy, but some jurisdictions have crafted regulations that address virtual currency-based financial services. The fact that some states are being proactive is encouraging, but the piecemeal approach being taken has created substantial differences in licensing requirements state-by-state. For example, virtual currency falls within the statutory definition of "Money Transmission" and is subject to licensing requirements in Washington State. On the contrary, New Hampshire specifically exempted from virtual currency from money transmission regulation.[98] Some states, like Colorado, have just taken up the issue now in the current legislative term.[99]

Money transmission licensing can be very expensive, and the differences in regulatory compliance requirements across jurisdictions can be costly and confusing for blockchain currency transfer businesses. Two of the most popular businesses that allow users to transmit Bitcoins, Coinbase and Circle, have each reported that they spent approximately $2 million and several years to secure money transmission licenses in only 25 states.[100] Even if some states adopt clear policies for the exchange of blockchain currencies within their borders, inconsistency across jurisdictions could create ongoing

[96] 15 U.S.C. § 1693a(7)(B) (2017).

[97] *See* Consumer Financial Protection Bureau, *supra* note 93 (New CFPB rules creating mandatory disclosures regarding remittance fees and exchange rates associated with international transfers may impact blockchain currency transactions, which have unique benefits when used to transfer remittances, but this relationship is tangential to overall virtual currency use.); *see* 12 C.F.R. § 1005 (2017).

[98] 19 R.C.W. Ch. 19.230; H.B. 436, 2017 Leg., Reg. Sess. (NH. 2017).

[99] H.B. 1220, Leg., Reg. Sess. (CO.2018).

[100] INTERNAL REVENUE SERV., Notice 2014-21, 48.

challenges for blockchain currency businesses working to achieve full regulatory compliance.[101]

Last year, the Supreme Court of New York upheld the State's Financial Services Law, one of the first state laws directly regulating virtual currency. [102] The New York Law gives the state's financial services department broad authority to regulate financial products and services, including virtual currency money businesses.[103] Early in 2018, New York legislators proposed an amendment to this law to allow state agencies to accept cryptocurrencies as payment for public services and fees.[104] The Arizona Senate passed a similar bill on February 8, 2018 proposing to allow residents to pay state taxes using cryptocurrencies,[105] as did the Illinois General Assembly on February 15, 2018.[106]

In a relatively bold move, a Vermont State Senator introduced a bill last month authorizing the creation of digital currency limited liability companies formed to operate digital currency systems in Vermont. The state would tax these new companies $0.01 for each unit of cryptocurrency that is mined, created, sold, or transferred in the state.[107] Although the bill is unlikely to pass, it represents the degree to which some states are welcoming cryptocurrency and the economic activity it fosters.

Some states have been eager to adopt virtual currencies within their borders. However, this does not mean that state financial regulators are taking a backseat. Tennessee is currently considering a law that would prohibit trustees of pensions or retirement benefit funds from investing in cryptocurrency assets.[108] Similarly, financial regulators in both Texas and North Carolina have initiated enforcement actions against Bitconnect, a cryptocurrency exchange that planned to launch an ICO in January 2018.[109] Unexpectedly, the exchange shut down just a few days after the agencies initiated these actions. According to a class action suit filed against Bitconnect on behalf of the investors whose money disappeared when the exchange closed, Bitconnect perpetrated several frauds, schemes, and violations of U.S. securities law.[110]

This regulatory action occurred on the heels of SEC's resolution of the *Munchee* enforcement action, and is a good indication many states will be following the federal regulator's stronger law enforcement policies. While

[101] *Id.* at 52-55.

[102] Chino v. New York Department of Financial Services, 2017 N.Y. Misc. LEXIS 5153 (N.Y. App. Div. Dec. 21, 2017).

[103] N.Y. Fin. Serv. Law §§ 101-608 (Consol. 2011).

[104] A.B. 9782, 241st Leg. (N.Y. 2018).

[105] S.B. 1091, 53rd Leg., 2d Reg. Sess. (Ariz. 2018).

[106] H.B. 5335, 100th Gen. Assemb., Reg. Sess. (IL. 2018).

[107] S.B. 269, 74th Biennial Sess. (VT. 2018).

[108] H.B. 2093, 2017 Leg., 241st Sess. (Tenn. 2018).

[109] In the Matter of BitConnect, Dkt No. 17 SEC 091 (N.C. Jan. 9, 2018); In the Matter of BitConnect, Dkt No. ENF-18-CDO-1754 (Tex. Jan. 4, 2018).

[110] Charles Wildes et al v. Bitconnect International et al., Dkt. No. 9:18-cv-80086-DMM (S.D. FL Jan. 24, 2018).

states will take their positions regarding cryptocurrency based on what they believe is best for their residents, virtual currency investors should be on the lookout for increased state-level regulation across the board. Recently, the National Conference of Commissioners on Uniform State Laws (or the "Uniform Law Commission") voted to approve a model act addressing digital currencies. Among other things, the Uniform Regulation of Virtual Currency Businesses Act ("Uniform Act") protects consumers by requiring cryptocurrency exchanges to maintain enough virtual currency to cover all user accounts. The model act also protects users of a cryptocurrency exchange from having their accounts confiscated by the creditors of the exchange. The Uniform Act applies only in the absence of adequate law or regulation of virtual currency businesses, so states remain free to create their policies even if they adopt the model act.[111] Now that the Uniform Law Commission has approved the Uniform Act, it will be submitted to the state legislatures for adoption. If most or all jurisdictions adopt the model act, virtual currency businesses may face less of a burden when it comes to cross-jurisdictional compliance.

VI. SELF-REGULATION AND CORPORATE POLICIES IMPACTING CRYPTOCURRENCY MARKETS

Despite the push to create a uniform regulatory policy regarding virtual currencies, the current executive administration is not at all favorable to economic controls. In fact, given the new executive order restricting administrative agencies, it is possible that the federal financial regulators will have their hands tied.[112] However, many cryptocurrency market participants are hungry for regulation, which is widely believed to be necessary before virtual currencies can fully enter the realm of mainstream finance. As a result, private actors have been working to curb some of the market abuses and other issues impacting cryptocurrency investors.

There has been some promising recent movement in the self-regulation of cryptocurrency companies. For example, technology thinktank Protocol Labs developed a Simple Agreement for Future Tokens ("SAFT") in October 2017 to address the legal uncertainty surrounding ICOs. The SAFT is meant to serve as an investment agreement between an ICO organizer and its investors that ensures the coin sale is compatible with U.S. securities law. It essentially acts as an option to purchase that is valid until the launch of the coin platform, at which time investors can call in the option in exchange for new

[111] National Conference of Commissioners on Uniform State Laws, *Uniform Regulation of Virtual Currency Business Act* (July 19, 2017) http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2017AM_URVCBA_AsApproved.pdf.

[112] *See generally* Proclamation No. 13771,, 82 Fed. Reg. 9,339 (Feb. 3, 2017)..

coins. Protocol Labs used the SAFT to launch its token sale last year and has since developed it into a working model for self-regulation.[113]

Similarly, the Chamber of Digital Commerce formed the Token Alliance to encourage best practices for startups seeking to raise capital through ICOs. This initiative is meant to promote responsible ICOs through industry-led policy development. The Token Alliance had over 70 founding members when it launched in late September 2017, and it remains open to all industry participants.[114]

The cryptocurrency industry is not alone in its efforts to foster private regulation of ICOs and virtual currency investment. Facebook, which is among the world's largest digital advertising companies, banned ICOs and cryptocurrency-related ads from its site in late January 2018. According to the company, it created the new policy because these advertisements are "frequently associated with misleading or deceptive promotional practices."[115] While the decision has attracted some criticism as inappropriate corporate censorship, at its core Facebook's policy is a consumer protection measure. Until financial regulators can curb the fraud and abuse that the company has rightly pointed to as the reasoning behind its new policy, the ban is likely to remain in place.

Just a few days after Facebook announced its new policy regarding ICOs and virtual currency ads, several large U.S. banks decided that they too needed to do something to shield themselves and their customers from cryptocurrency risks. JPMorgan Chase, Bank of America, and CitiGroup all announced that they would no longer authorize credit card purchases from cryptocurrency exchanges. Likewise, Capital One and Discover also decided to ban cryptocurrency purchases starting in January 2018.[116] These prohibitions are likely to be temporary, but U.S. banks are responding to legitimate concerns regarding theft, fraudulent transfers, and irresponsible speculation on cryptocurrency investments. Like the Facebook ban, these policies will almost certainly remain in place until financial regulators step in.

[113] Protocol Labs, *Announcing the SAFT Project* PROTOCOL.AI (Oct. 2, 2017) https://protocol.ai/blog/announcing-saft-project/.

[114] Chamber of Digital Commerce, *Blockchain Industry and Regulatory Leaders Launch Token Alliance* (Sept. 18, 2017) https://digitalchamber.org/blockchain-industry-and-regulatory-leaders-launch-token-alliance/.

[115] Rob Leathern, *New Ads Policy: Improving Integrity and Security of Financial Product and Services Ads, Facebook Business* (Jan. 30, 2018) https://www.facebook.com/business/news/new-ads-policy-improving-integrity-and-security-of-financial-product-and-services-ads.

[116] Evelyn Cheng, *JPMorgan Chase, Bank of America & Citi bar people from buying bitcoin with a credit card* CNBC (Feb. 2, 2018) https://www.cnbc.com/2018/02/02/jpmorgan-chase-bank-of-america-bar-bitcoin-buys-with-a-credit-card.html.

VII. CONCLUSION AND POLICY RECOMMENDATIONS

Blockchain currencies may have a groundbreaking impact on financial transaction norms of the internet. While this technological innovation does not fit squarely within any single U.S. regulatory regime, several of the federal and state agencies with jurisdiction over virtual currencies have clarified their policies regarding compliance, enforcement, and application of existing rules. The law surrounding virtual currency has developed quickly, but regulators are still struggling to keep up with the constantly-changing landscape of crypto-based financial products and services. As new issues continue to arise, we can expect to see increasing regulation aimed at addressing the taxation, consumer protection, and financial crime issues raised by this exciting new technology.

Overall, regulators are struggling to develop a coordinated approach to cryptocurrency markets. In the meantime, however, major enforcement actions continue to grab headlines. Cryptocurrency-based financial crimes enforcement has become increasingly robust over the past few months. Federal agencies are taking a bold stance, offering further evidence that, despite the lack of a uniform set of laws that apply to cryptocurrency markets, the government is doing everything that it can to reign in fraud and abuse. Self-regulation and private sector consumer protection policies have also arisen in response to growing demand for controls on the ever-volatile virtual currency markets, with a particular eye towards curbing fraud among unscrupulous ICOs. All in all, cryptocurrency market participants can expect to see more rules and regulation imposed upon a formerly free market.

The substantial concern over the potential criminal uses of blockchain currencies has triggered widespread law enforcement activities. Regulators should not restrict the use of this technology just because of its potential for use in illicit online activities. Like cash, the legitimate uses of blockchain currencies far outweigh criminal uses. Doing so would unnecessarily burden the technology and may suppress critical innovation in the future.[117]

Policy clarifications by the Securities and Exchange Commission, Commodities Futures Trading Commission, the Financial Crimes Enforcement Network, the Internal Revenue Service, and the financial regulatory bodies of several states have helped work blockchain currencies into existing regulatory frameworks. These organizations have addressed rules regarding virtual currency transactions, securities exchanges, derivatives markets, domestic payment processing, and remittances all in a relatively short period, although additional information is sure to become known as current enforcement and administrative actions unfold. Also, jurisdictional differences in state money transmission licensing requirements

[117] *See* Brito, *supra* note 1 at 67-68 (describing, because blockchain currencies are decentralized, it is questionable whether it is even possible to control peer-to-peer sharing to a meaningful degree).

create costly and duplicative compliance procedures for businesses affected by these rules.

To avoid this inefficiency, states could develop license reciprocity agreements, allow for license-sharing arrangements, and create uniform cross-jurisdictional licensing allowances.[118] State lawmakers have already shown progress in this regard with the development of the Uniform Act, which represents an early attempt to address some of the extraterritorial regulatory issues raised by cryptocurrency transactions. However, rather than waiting for slowly-developing bureaucratic solutions, the cryptocurrency market is developing a system of self-regulation. As a result, the private sector is beginning to establish a system to normalize activities in cryptocurrency markets as public agencies work towards establishing uniform national policies.

[118] *Id.* at. 53-54 (Federal preemption of state currency exchange licensing may also be possible, although likely not politically tenable.); s*ee also id.* at 71.

***