REGULATING THE UNREGULATABLE: THE DIGITAL COMMODITY EXCHANGE ACT’S USE-BASED APPROACH TO CRYPTOCURRENCY REGULATION

BEGGY POWELL*

Abstract: Since the creation of Bitcoin in 2008, the cryptocurrency market has grown exponentially and remained relatively free from government oversight. Only within the last five years have federal agencies begun to regulate the risks the industry poses. Their response to date, though, has been piecemeal because they lack explicit, statutory jurisdiction over the industry. As a result, the cryptocurrency market faces several risks that threaten to derail its future growth. For one, the industry is a playground for criminal activity, including everything from money laundering to fraud to cyberattacks. The market is also extremely volatile, and consumers have little understanding of the underlying technology in which they are investing. Furthermore, the industry is in its early stages and has not yet developed mechanisms to mitigate these risks. Commentators initially rejected government interference out of fears it would chill the industry’s development. Now, they are increasingly calling for Congress to provide guidance. Congress has proposed a few bills, the most recent by Congressman Michael Conaway (TX-11). Conaway’s bill, the Digital Commodity Exchange Act, would give the Commodity Futures Trading Commission explicit jurisdiction over cryptocurrency when used as a commodity. Although the bill is imperfect, it presents a potential path forward for Congress and the industry. Similar legislation that grants federal agencies jurisdiction over cryptocurrency based on how it is used would create the regulatory flexibility and societal trust that the industry needs to continue to develop successfully.

INTRODUCTION

The global economy has not seen a technology that could potentially disrupt the current markets as much as cryptocurrency since the introduction of the internet.¹ In 2008, the mysterious Satoshi Nakamoto created the original cryptocurrency, Bitcoin, specifically to provide a currency outside the scope of

¹ See Kevin Werbach, Trust, But Verify: Why the Blockchain Needs the Law, 33 BERKLEY TECH. L.J. 487, 496–97 (2018) (noting how Bitcoin and blockchain has created an excitement in the technology industry not seen since the advent of the internet).
traditional financial institutions. Investors flocked to this new form of currency, attracted by its potential to disrupt current payment systems and take them completely outside the hands of government. Since then, the cryptocurrency market has exploded, with thousands of different cryptocurrencies available around the globe.

The development of the cryptocurrency market mirrors the myriad of different use-based internet services that have developed since the internet’s creation but is focused on the finance industry. Some cryptocurrencies, like Bitcoin and Litecoin, are specifically designed to serve as substitutes for government-issued money. Others, like Ethereum and Cardano, were founded to create completely decentralized financial systems for people without access to traditional financial products. Alternatively, some strive to make improvements to the current financial system, such as Stellar, which allows certain large transactions between institutions to occur instantaneously rather than after a few days. Consumers have used these cryptocurrencies for a variety of traditional financial purposes, including traditional monetary transactions, investment in commodities and securities, and smart contracts.

2 Daniela Sonderegger, A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation, 47 Wash. U. J. L. & Pol’y 175, 180–81 (2015); see Werbach, supra note 1, at 498 (noting that Nakamoto is a pseudonym).

3 Kevin V. Tu & Michael W. Meredith, Rethinking Virtual Currency Regulation in the Bitcoin Age, 90 Wash. L. Rev. 271, 274 (2015).


5 See Werbach, supra note 1, at 529–30 (comparing the issues regulators had with classifying internet services to cryptocurrencies). A use-based internet service refers to the different categories of companies that provide internet services. Id. For example, Verizon provides telecommunication services, and YouTube provides entertainment services. Id. at 529; Avery Minor, Cryptocurrency Regulations Wanted: Iterative, Flexible, and Pro-Competitive Preferred, 61 B.C. L. Rev. 1149, 1154 (2020). Because these companies can provide a variety of different internet services, they do not fit into regulatory category. Werbach, supra note 1, 529–30. For example, Amazon traditionally provided only eCommerce services but now also supports voice messages through its personal assistant device Echo, potentially qualifying it as a telecommunication carrier. Id. at 529. Cryptocurrency has a similar problem because some cryptocurrencies can act as replacements for government-backed money and serve as a form of investment. See Tu & Meredith, supra note 3, at 273 (discussing Bitcoin as both a replacement for government-backed money and as a security); Werbach, supra note 1, at 530 (noting that regulators are still determining when certain regulations apply to different cryptocurrency transactions).


7 Id. A decentralized financial system allows the public to access financial products without going through a middleman, such as a bank or brokerage. Rakesh Sharma, Decentralized Finance (DeFi) Definition, INVESTOPEDIA (June 6, 2021), https://www.investopedia.com/decentralized-finance-defi-5113835. This system usually operates through a public software written on blockchains that are not controlled by these middlemen and do not require a form of identification to access, such as a government-issued ID. Id.

8 Conway, supra note 6.

Cryptocurrency’s various potential uses, its anonymity, and its lack of cumbersome red tape caused individuals to rush to invest in this new technology.\textsuperscript{10} This influx of initial attention, though, also created substantial market volatility.\textsuperscript{11} On top of this instability, cryptocurrency has been a boon for criminal activity, including money laundering, tax evasion, and crypto hacks, which have raised serious consumer protection concerns in the industry.\textsuperscript{12}

Now, in a turnabout face, industry experts are increasingly calling for the federal government to pass comprehensive cryptocurrency regulation.\textsuperscript{13} In response, Congressman Michael Conaway (TX-11) introduced the Digital Commerce Exchange Act (DCEA) to provide the Commodity Futures Trading Commission (CFTC) with jurisdiction to regulate cryptocurrency.\textsuperscript{14} However, Congress would also need to pass additional legislation, similar to the DCEA, that grants other federal agencies jurisdiction over cryptocurrency through a use-based approach to ultimately achieve the DCEA’s goal.\textsuperscript{15}

Part I of this article provides background on cryptocurrency and the current regulatory framework for cryptocurrency in the United States.\textsuperscript{16} It then discusses recent legislation introduced in Congress to improve this framework, including the DCEA.\textsuperscript{17} Part II surveys some of the major risks to the cryptocurrency market and the provisions of the DCEA that try to address those risks when cryptocurrency is used as a commodity.\textsuperscript{18} Finally, Part III examines where the DCEA achieved its goals and where it falls short and suggests that Congress should regulate cryptocurrency based on how consumers use it within the market.\textsuperscript{19}

\textbf{I. Regulation of Cryptocurrency in the United States: A Piecemeal Approach}

6. A smart contract is a contract between a buyer and seller written into code. Jake Frankenfield, \textit{Smart Contracts}, \textsc{Investopedia} (May 26, 2021), https://www.investopedia.com/terms/s/smart-contracts.asp. The code will carry out the transaction, and the transaction is completely traceable, transparent, and irreversible. Id. Smart contracts allow parties to ensure that a transaction will occur without relying on a trusted intermediary, such as the government. Id.

10 Tu & Meredith, \textit{supra} note 3, at 273–75.

11 See id. at 337 (noting the Bitcoin’s price volatility reminds commentators of “the ‘Wild West’ facing investors prior to the passage of the Securities Act of 1933”).

12 Tyler C. Lee, \textit{Decrypting Crypto: Issues Plaguing Today’s Hottest Regulatory Nightmare}, 16 \textsc{N.Y.U. J.L. & BUS.} 551, 558, 569 (2020). A crypto hack occurs when someone steals cryptocurrency by infiltrating the network used to store it. Id. at 558. For example, in 2018, a South Korean digital exchange lost thirty percent of its digital assets when someone hacked its network. Id.

13 John W. Bagby et al., \textit{An Emerging Political Economy of the Blockchain: Enhancing Regulatory Opportunities}, 88 \textsc{U. Mo. Kan. City L. Rev.} 419, 421 (2019); Werbach, \textit{supra} note 1, at 532.


15 Press Release, House Comm. on Agric. – Republicans, 116\textsuperscript{th} Cong., Summary of the Dig. Commodity Exch. Act of 2020 at 1; see discussion \textit{infra} notes 163–260 and accompanying text.

16 See discussion \textit{infra} notes 20–84 and accompanying text.

17 See discussion \textit{infra} notes 20–84 and accompanying text.

18 See discussion \textit{infra} notes 85–162 and accompanying text.

19 See discussion \textit{infra} notes 163–260 and accompanying text.
The cryptocurrency market currently suffers from a disjointed regulatory framework. Congress and federal agencies have struggled to define cryptocurrency and to regulate it to promote innovation, prevent criminal activity, and protect consumers. Although states have taken a myriad of approaches, Congress has largely deployed a wait and see approach over the past ten years, leaving federal agencies responsible for regulating cryptocurrency. This strategy has changed within the last few years, as Congress has repeatedly introduced new legislation in an attempt to meet industry demand. The DCEA is one of the most recent attempts to provide federal agencies with more clear authority to regulate cryptocurrencies.

Section A of this Part defines cryptocurrency and the underlying technology that makes cryptocurrency transactions possible. Next, Section B of this Part provides an overview of the current federal regulatory framework for cryptocurrency, starting with the CFTC. Section C of this Part examines how the Securities and Exchange Commission (SEC) has historically treated cryptocurrency in comparison to the CFTC’s treatment of cryptocurrency. Section D then explores what other agencies have exercised jurisdiction over cryptocurrency within the Department of Treasury. Finally, Section E of this Part discusses recent attempts by Congress to regulate the cryptocurrency market, including the DCEA.

### A. What is Cryptocurrency?

The foundation of cryptocurrency is distributed ledger technology, with the blockchain technology used in Bitcoin serving as the most common version. This technology obtained public notoriety after Bitcoin’s launch in 2008 and provides the same function for cryptocurrency that the internet provides for websites.

---

20 Lee, supra note 12, at 560.
21 See id. (discussing how the lack of a federal definition for cryptocurrency has made companies uncertain about how to comply with the current piecemeal legal framework).
22 Id.; Scott D. Hughes, Cryptocurrency Regulations and Enforcement in the U.S., 45 W. ST. L. REV. 1, 21 (2017).
25 See discussion infra notes 30–47 and accompanying text.
26 See discussion infra notes 48–56 and accompanying text.
27 See discussion infra notes 57–68 and accompanying text.
28 See discussion infra notes 69–75 and accompanying text.
29 See discussion infra notes 76–84 and accompanying text.
30 Dennis Chu, Broker-Dealers for Virtual Currency: Regulating Cryptocurrency Wallets and Exchanges, 118 COLUM. L. REV. 2323, 2326 (2018); Jake Frankenfield, Cryptocurrency, INVESTOPEDIA (May 5, 2020), https://www.investopedia.com/terms/c/cryptocurrency.asp. Blockchain is a type of distributed ledger that organizes and verifies transactions in groups called “blocks” when recording them on the ledger. Emily Rutland, Blockchain Byte, FIN. INDUS. REGUL. AUTH., https://www.finra.org/sites/default/files/2017_BC_Byte.pdf (last visited Feb. 5, 2021). One of the benefits of blockchain as a distributed ledger is that its verification process ensures that users can trust that a transaction will take place without having to trust the individuals involved in the transaction. Werbach, supra note 1, at 491; Rutland, supra note 30.
31 Werbach, supra note 1, at 498; see id. at 521 (comparing the structure, use, and potential of blockchain to the internet).
Distributed ledger technology is the basis from which cryptocurrencies are created and how customers interact with them.\textsuperscript{32} A distributed ledger is a consensually shared, usually decentralized, digital ledger that records digital asset ownership and sales, similar to a land registry.\textsuperscript{33} Every transaction is recorded on the ledger, and users with access to the ledger can see every transaction.\textsuperscript{34} Those conducting the transactions, though, are generally outwardly anonymous, and transactions on a blockchain ledger are impossible to reverse.\textsuperscript{35} The goal of these ledgers is to provide cryptocurrency users with a distributed, accurate ledger that does not require a central administrator.\textsuperscript{36} Decentralized ledgers, however, cannot distinguish between customers making legitimate transactions and customers engaging in criminal activity.\textsuperscript{37} Moreover, blockchain in particular has no mechanism to prevent or reverse theft from a fraudulent transaction.\textsuperscript{38}

Bitcoin and other cryptocurrencies are digital assets recorded on these distributed ledgers, which people obtain by accepting them as a form of payment, buying them with government-issued currency on an exchange, or mining or creating the digital assets.\textsuperscript{39} Users have their own private key to access their cryptocurrencies and conduct transactions on the ledger.\textsuperscript{40} As of May 2020, the market offered over 5,000 cryptocurrencies.\textsuperscript{41} Bitcoin is the most commonly used cryptocurrency, holding over sixty percent of the cryptocurrency market share.\textsuperscript{42}

\textsuperscript{32} Chu, \textit{supra} note 30, at 2326.
\textsuperscript{33} Id.
\textsuperscript{34} Rutland, \textit{supra} note 30.
\textsuperscript{35} Chu, \textit{supra} note 30, at 2326. Different cryptocurrencies and their underlying distributed ledger technology offer various levels of anonymity to users. Shobhit Seth, \textit{6 Private Cryptocurrencies}, \textit{INVESTOPEDIA}, https://www.investopedia.com/tech/five-most-private-cryptocurrencies/ (July 4, 2021); see also Danny Bradbury, \textit{How anonymous is Bitcoin?}, \textit{COINDESK} (June 7, 2013), https://www.coindesk.com/how-anonymous-is-bitcoin (discussing how Bitcoin transactions are pseudo-anonymous and how big data companies and law enforcement can trace these transactions).
\textsuperscript{36} Werbach, \textit{supra} note 1, at 491–503.
\textsuperscript{37} E.g., id. at 492–93 (noting that a blockchain platform’s inability to distinguish between criminal activity and legitimate transactions allowed thieves to siphon funds from the system).
\textsuperscript{38} Id. at 491.
\textsuperscript{39} Chu, \textit{supra} note 30, at 2326; Stephen Wilks, \textit{The Reimagined Schoolyard: Cryptocurrency’s Adoption in Tomorrow’s International Monetary Order}, 2020 B.C. INTELL. PROP. & TECH. F. 1, 34 (2020). Bitcoin is the most well-known cryptocurrency that requires mining. Tu & Meredith, \textit{supra} note 3, at 273, 281. For Bitcoin, mining both creates Bitcoins and verifies transactions. Kelsey L. Penrose, \textit{Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Law}, 18 N.C. BANKING INST. 529, 531 (2014). Anyone can become a miner by downloading software to connect to Bitcoin’s network and forming a “node.” Id. at 531–32. When someone transacts in bitcoin, it sends out a signal to this network, and the miner’s node collects the transactions, puts them into “blocks,” verifies the transactions in the block by solving a complex algorithm, and then records the transactions in the block on the ledger. Id. at 532, 533. Every time one of these blocks are published, the network creates bitcoins and gives them to the miners. Id. at 533. Miners also receive bitcoins through transaction fees. Id.
\textsuperscript{40} Chu, \textit{supra} note 30, at 2326.
\textsuperscript{41} Wilks, \textit{supra} note 39, at 34.
\textsuperscript{42} Id.
Most cryptocurrency trading is done on exchanges, where customers trade cryptocurrency for other cryptocurrencies or for government issued currency. These exchanges vary in fees and the tradable assets they offer. Customers must hold a digital wallet with an exchange to access its services. Digital wallets are services that store and protect cryptocurrency for owners. These services operate as custodians to customers’ private keys, and customers do not have access to these private keys.

B. The CFTC’s Regulation of Cryptocurrency

Cryptocurrencies used as a commodity fall under the CFTC’s jurisdiction. The CFTC oversees derivative transactions involving commodities under the Commodity Exchange Act. Commodities are “goods and articles . . . and all services, rights and interests . . . in which contracts for future delivery are presently or in the future dealt in.” The agency has taken the stance that cryptocurrency is a commodity, and, therefore, is under its jurisdiction. The CFTC has also been one of the most active federal agencies in enforcing its jurisdiction and providing information to the public on cryptocurrency. In September 2015, the CFTC became one of the first regulators to bring an action against a cryptocurrency company when it went after Coinflip, a company that connected customers with Bitcoin options and futures contracts. The CFTC charged Coinflip with not following CFTC regulations for trading commodity options and for not properly registering its facility with the agency. The District Court for the Eastern District of New York upheld the Commission’s decision, determining that the CFTC had the power to police fraud and market manipulation in cryptocurrency. In the following years, the CFTC has issued further guidance on cryptocurrencies and publicly sought to deliver a more unified message around cryptocurrencies with the SEC and the Financial Crimes Enforcement Network (FinCEN).

43 Chu, supra note 30, at 2328.
44 Id.
45 Id. at 2329.
46 Id. at 2327.
47 Id. at 2327–28.
49 Commodity Exchange Act 7 U.S.C. § 2; Minor, supra note 5, at 1160.
52 See Bitcoin, Commodity Futures Trading Comm’n, https://www.cftc.gov/Bitcoin/index.htm (last visited Nov. 13, 2020) (discussing the CFTC’s definition of digital assets and advising consumers to use caution when trading in digital assets); Commodity Futures Trading Comm’n, supra note 51.
54 Id.
C. The SEC’s Regulation of Cryptocurrency

In comparison, the SEC has only in the past few years taken a more active role in regulating securities that involve digital assets.\(^{57}\) The agency considers whether a digital asset is a security as a fact based inquiry.\(^{58}\) Securities are generally a financial instrument traded for speculation or investment, such as investment contracts, bonds, treasury stock, and foreign currency.\(^{59}\) Cryptocurrencies are considered securities when they function like investment contracts.\(^{60}\) An investment contract is a transaction where someone invests money in an entity to gain a profit but relies predominately on a third party to manage and run the entity.\(^{61}\)

Unlike the CFTC and cryptocurrency commodities, a federal district court, not the SEC, was the first to consider cryptocurrency as a security publicly.\(^{62}\) In 2013, in Securities Exchange Commission v. Shavers, the District Court for the Eastern District of Texas took that first step when it categorized cryptocurrency as a security in dicta.\(^{63}\) In 2017, the SEC released an investigative report that officially concluded cryptocurrency could function as a security and advised companies that used blockchain or other distributed ledgers to take appropriate steps to comply with all securities laws.\(^{64}\)

Since the report’s release, the SEC has taken a more active role in cryptocurrency regulation.\(^{65}\) For example, the SEC has launched investigations and brought enforcement proceedings against companies whose initial coin offerings (ICOs) counted as unregistered offerings and sales of securities.\(^{66}\) The SEC has also released guidance that trading platforms of digital assets may count as securities exchanges.\(^{67}\) The agency has further forbidden companies from linking exchange

---


\(^{60}\) Beugelmans & Hess, supra note 57.

\(^{61}\) Howey, 328 U.S. at 298–99.


\(^{63}\) See generally Beugelmans & Hess, supra note 57.


\(^{65}\) Shavers, 2013 WL 4028182 at *2.
traded funds to cryptocurrencies because of uncertainty surrounding the practice’s compliance with the Investment Company Act of 1940, which requires exchange traded funds that qualify as investment companies to register with the SEC.68

D. The Regulation of Cryptocurrency by Other Federal Agencies

FinCEN, the Office of the Comptroller of Currency (OCC), and the Internal Revenue Service (IRS), all bureaus of the Department of Treasury, also regulate cryptocurrency.69 FinCEN regulates the financial markets to prevent criminal activity such as money laundering.70 In 2013, FinCEN announced that sellers and exchangers of Bitcoin counted as money transmitters under the Bank Secrecy Act, and consequently, must implement monitoring systems to prevent and report money laundering and other criminal activity.71 The OCC, the primary U.S. bank regulator, has also taken steps to issue guidance on cryptocurrency.72 For example, it has classified cryptocurrency custody services, such as holding the unique key associated with a cryptocurrency, as traditional banking activities.73 Since 2016, the IRS has provided additional guidance that tax payers should count the sale of cryptocurrency as a capital gain or loss for tax purposes.74 Although these agencies along with the CFTC and SEC are the main cryptocurrency regulators, other federal agencies, such as the Federal Trade Commission and the Department of Justice, also have been involved in cases of consumer fraud and criminal activity related to cryptocurrency.75

E. Congress’s Attempts to Bring Coherency to Cryptocurrency Regulation

In March 2020, Congressman Paul Gosar introduced the Crypto-Currency Act in an attempt to bring some coherency to this regulatory framework.76 The bill’s stated purpose is “to clarify which Federal agencies regulate digital assets, to require those agencies to notify the public of any Federal licenses, certifications, or

---

68 The Investment Company Act of 1940 15 U.S.C. §§ 80a-1 to 80a-64 (1940); Beugelmans & Hess, supra note 57; Engaging on Fund Innovation and Cryptocurrency-related Holdings, supra note 57. An exchange traded fund (ETF) is a type of security that holds multiple underlying assets, such as commodities, bonds, stocks, or a mixture of assets, to track a certain index, sector, or other asset. James Chen, Exchange Traded Fund, INVESTOPEDIA, https://www.investopedia.com/terms/e/etf.asp (Mar. 3, 2021). For example, a bond ETF may include federal, state, and municipal bonds, an industry ETF may track the technology or banking industry, and a commodity ETF may invest in commodities such as gold or oil. Id. Like stocks, ETFs are traded on an exchange through online or traditional broker-dealers. Id.

69 Hughes, supra note 22, at 13, 19, 27.

70 Bagby, supra note 13, at 444–45.


73 Id.


75 Hughes, supra note 22, at 16, 20.

76 H.R. 6154.
registrations required to create or trade such assets, and for other purposes.”77 The bill is short and mainly seeks to accomplish its goal by defining “crypto-commodity,” “crypto-security,” and “crypto-currency.”78 Additionally, the bill assigns jurisdiction to the relevant agencies, the CFTC, the SEC, and the Department of Treasury acting through FinCEN and the Comptroller of Currency, respectively.79

On September 24, 2020, Congressman Conaway provided another solution when he introduced the DCEA to the House Committee on Agriculture.80 In a public statement, Conaway expressed his hope that the bill would close the hole in regulation between the CFTC and the SEC and provide an alternative to various state regulations for exchanges.81 Rather than attempting to provide jurisdiction to a group of agencies, the DCEA intends only to grant the CFTC jurisdiction over cryptocurrencies that act as a “digital commodity” as an amendment to the Commodity Exchange Act.82 Congressman Conaway believes the bill serves the interests of both companies and consumers.83 Additionally, Congressman Conaway aims to harmonize state and federal regulatory frameworks, provide greater consumer protection, and make compliance easier by simplifying and clarifying cryptocurrency’s legal status.84

II. RISKS TO THE CRYPTOCURRENCY MARKET AND THE DCEA

Congress will have to balance the need to prevent criminal activity, protect consumers, and the desire to promote innovation in the cryptocurrency market to improve the existing piecemeal regulatory framework.85 The cryptocurrency market is rife with illicit activity, including money laundering, fraud, and large-scale theft.86 Consumers are largely unaware of the scale of these issues and are exposed to outsized risk when investing due to their unfamiliarity with the technology and lack of access to meaningful information about cryptocurrency providers.87 The current piecemeal framework and uncertainty around future legislation have impeded the market’s response because cryptocurrency developers, sellers, and buyers focus on how to lawfully operate rather than addressing these risks.88

77 Id.
78 H.R. 6154 § (2)(1)–(3).
79 Id. at § (2)(8).
80 See generally House Comm. on Agric. – Republicans, supra note 24.
81 Id. at 1.
82 H.R. 8373 § 2(b); H.R. 6154 § 3.
83 House Comm. On Agric. – Republicans, supra note 24, at 1.
84 Id.
85 John W. Bagby et al., An Emerging Political Economy of the Blockchain: Enhancing Regulatory Opportunities, 88 U. MO. KAN. CITY L. REV. 419, 449 (2019); Adam J. Kuegler, Cryptocurrency and the SEC: How a Piecemeal Approach to Regulating New Technology Selectively Stifles Innovation, 52 CONN. L. REV. 989, 1009 (2020) (arguing that because federal agencies have a higher rate of policymaking than Congress, they are better suited to handle quickly changing technology).
86 Bagby, supra note 85, at 440.
The DCEA attempts, in part, to solve some of these issues and stabilize the market when cryptocurrency is used as a commodity. First, it provides definitions to describe the market for digital commodities in an attempt to establish clearer boundaries for when cryptocurrency is a commodity. It then attempts to define the CFTC jurisdiction over digital commodity transactions. Finally, it provides mechanisms to lawfully establish and maintain digital commodity exchanges to prevent criminal activity and protect consumers.

Section A of this Part examines the current risks to the development of the cryptocurrency market from within the industry and from the government. Section B of this Part then explores the DCEA and its regulatory mechanisms that attempt to address these risks when cryptocurrency is used as a commodity.

A. Current Risks to the Cryptocurrency Market

The cryptocurrency market faces two obstacles to its incorporation into the economy: widespread illicit activity and consequent overbearing regulation. Subsection 1 discusses the challenge of illicit activity and mismanagement of cryptocurrency platforms, which creates mistrust amongst consumers and prevents wide scale adoption. Subsection 2 addresses the government’s attempts to prevent this illicit activity, which inhibits new companies from entering the industry and stifles innovation. The uncertainty created by these two challenges may limit the long term development of cryptocurrency and its usefulness to the economy.

1. Risks Inside the Industry: Bad Actors and Inexperience

The anonymous nature of cryptocurrency platforms allows users and developers to easily exploit them for criminal purposes. A 2018 study found that some $76 billion worth of Bitcoin transactions were connected to criminal activity, amounting to 25% of Bitcoin’s users and 46% of its total transactions. In addition to typical concerns about money laundering, another study in 2017 found that up to 80% of Initial Coin Offerings (ICOs) were scams. The nonreversible payments

91 Id. at § 2(b).
92 Id. at § 2(c)–(e).
93 See discussion infra notes 95–138 and accompanying text.
94 See discussion infra notes 139–162 and accompanying text.
95 Werbach, supra note 87, at 528; Lee, supra note 88, at 558.
96 See discussion infra notes 99–121 and accompanying text.
97 See discussion infra notes 122–138 and accompanying text.
98 See Lee, supra note 88, at 556, 558.
99 See Lee, supra note 88, at 558.
100 Id. at 558–59.
101 Id. at 556. For example, the SEC recently froze the assets of the cryptocurrency company PlexCorps and accused it of fraud. Adi Robertson, SEC charges alleged cryptocurrency scam with fraudulently raising $15 million, THE VERGE (Dec. 5, 2017), https://www.theverge.com/2017/12/5/16739348/sec-plexcorps-plexcoin-ico-scam-asset-freeze-charges. The SEC alleges that when soliciting investors, the company falsely claimed to have a team
systems of cryptocurrencies like Bitcoin, moreover, leaves consumers with little redress for correcting frauds. For instance, if a consumer pays a merchant for an item online and the item is not delivered, the consumer has no efficient remedy. If the merchant decides not to refund the customer, the customer cannot get their money back.

Moreover, because cryptocurrency exchanges operate so heavily through the internet, weaknesses in network security leave exchanges and their users’ digital wallets exposed to hacking and extreme market volatility. In 2014, Mt. Gox, one of the most prominent Bitcoin exchanges at the time, collapsed after hackers stole close to $400 million in currency. In 2018, hackers stole 30% of the assets belonging to the South Korean exchange Conrail, causing the Bitcoin market to drop by 7% and erasing billions of dollars globally. These cyberattacks caused major financial institutions to remain wary of adopting cryptocurrency as a mainstream investment.

Additionally, consumers have few courses of redress if a hack occurs due to the current regulatory approach to cryptocurrency and the industry’s youth. The relative novelty of cryptocurrency platforms means that most providers are inexperienced and unsophisticated in the market. The general lack of government regulation in the industry allows for almost anyone to create cryptocurrency exchanges or ICOs. Some developers who initiate ICOs have little idea how to properly utilize the funds they receive. One study found that 45% of cryptocurrency exchanges have failed, and another found that 4% of ICOs failed as well.

ICO developers’ inexperience has meant that these cryptocurrency platforms often fail to adopt risk management measures, such as network security or password protections that would prevent costly mistakes. For example, when an employee of a cryptocurrency platform in Canada passed away, his customers
lost C$180 million worth of assets because he had stored them in an offline folder for which only he knew the password.\textsuperscript{115}

Investors in cryptocurrency also face an outsized exposure because of a lack of understanding of the underlying technology, in part due to the lack of transparency of cryptocurrency platforms.\textsuperscript{116} Cryptocurrency platforms traditionally are unregistered and do not share details about their operations.\textsuperscript{117} These platforms usually do not disclose how much of their customers’ assets they are holding, and, therefore, may not have enough cash in reserve to satisfy all claims if everyone withdraws their assets at once.\textsuperscript{118} This breeds doubt about how the platform will distribute money if the platform fails.\textsuperscript{119} Similarly, some ICOs have offered unfair terms to ordinary purchasers compared to the ICO’s developers without complete disclosure.\textsuperscript{120} Most customers have little experience with or understanding of the technology behind cryptocurrency, and this unfamiliarity, combined with the lack of transparency within the industry, leaves investors uninformed and unaware of the high risk level of their investment.\textsuperscript{121}

2. Risks from the Government: A Lack of Regulatory Strategy

Lack of government regulation will allow risks in the cryptocurrency market to fester.\textsuperscript{122} Improper government regulation, however, will also make it difficult for companies to operate and can stifle development.\textsuperscript{123} The piecemeal legal framework lacks explicit guidance or structure from Congress, government agencies, and states as they continue to determine the best legal approach.\textsuperscript{124} Cryptocurrency’s novelty often means it falls outside of or in between regulatory schemes.\textsuperscript{125} Ambiguity in the legal framework, though, may eventually drive startups out of business as they will be unable to afford continuous adjustments to changing regulations.\textsuperscript{126}

Commentators generally agree that the government needs to establish a regulatory framework for cryptocurrency, even if they do not agree about how it should look.\textsuperscript{127} For instance, some believe that the government cannot regulate

\textsuperscript{115} Stephen Wilks, The Reimagined Schoolyard: Cryptocurrency’s Adoption in Tomorrow’s International Monetary Order, 2020 B.C. INTELL. PROP. & TECH. F. 1, 40 (2020).
\textsuperscript{116} Werbach, supra note 87, at 519; Chu, supra note 110, at 2340.
\textsuperscript{117} Werbach, supra note 87, at 519; Chu, supra note 110, at 2340.
\textsuperscript{118} Chu, supra note 110, at 2340.
\textsuperscript{119} Id. at 2340–41.
\textsuperscript{120} Werbach, supra note 87, at 518.
\textsuperscript{121} Id. at 519; Chu, supra note 110, at 2324.
\textsuperscript{122} Chu, supra note 110, at 2358.
\textsuperscript{123} Bagby, supra note 85, at 422.
\textsuperscript{124} Kuegler, supra note 85, at 1025; Lee, supra note 88, at 577.
\textsuperscript{125} Bagby, supra note 85, at 448.
\textsuperscript{126} Kuegler, supra note 85, at 1026.
\textsuperscript{127} Compare Werbach, supra note 87, at 530, 531 (criticizing New York’s licensing system and calling for regulating cryptocurrencies similar to the internet), with Matthew Barrack, Current Regulators Overseeing Cryptocurrencies are Restricting Access to This Innovative New Technology, 26 PIABA B. J. 453, 480 (2019) (praising New York’s licensing system for providing a uniform regulatory system with less regulatory gaps for cryptocurrencies).
cryptocurrency, and that even if it could, it should refrain from doing so for now to promote innovation.\(^{128}\) They worry the government will artificially limit its development by categorizing it as something that it is not.\(^{129}\) Furthermore, they believe that less government regulation will help promote the technology’s development in the United States.\(^{130}\)

Others argue that a centralized approach would better promote the development of the cryptocurrency industry.\(^{131}\) One approach is for the federal government to create a specific agency dedicated to streamlining cryptocurrency regulation and facilitating startups’ compliance with the law.\(^{132}\) Contrastingly, the federal government could adopt a framework similar to New York, where any company using cryptocurrency in any manner must register for a license but remains subject to regulation from other federal agencies.\(^{133}\) Proponents of the licensing regime argue New York’s approach prevents money laundering, prescreens companies to prevent fraud, and ensures disclosure to the Internal Revenue Service.\(^{134}\) Others, however, believe that New York’s licensing system is too onerous and will restrict development, citing that only three companies were granted licenses from 2015 to early 2017.\(^{135}\)

Among those who believe the government should establish a strong regulatory framework for cryptocurrency, the general consensus is that Congress needs to provide explicit guidance through legislation.\(^{136}\) Explicit legislation, they argue, would address the current piecemeal approach that allows companies to exploit the system.\(^{137}\) Although these commentators may disagree on the form of that explicit legislation, they agree that it will create more stability in the cryptocurrency market by providing companies with clearer guidance for compliance and curtailing illicit activity.\(^{138}\)

**B. The Digital Commodities Exchange Act**

The DCEA attempts to tackle these problems by amending the Commodity Exchange Act to create clearer boundaries between the CFTC and the SEC and by establishing a regulatory framework that both facilitates trades of digital commodities and protects consumers.\(^{139}\) The DCEA begins by establishing the

---

128 Werbach, *supra* note 87, at 528.
129 *Id.* at 528, 529–30.
130 *See id.* at 520 (discussing how early internet developers and legal experts were “cyber-libertarians”).
131 *See, e.g.*, Kuegler, *supra* note 85, at 1026 (arguing that the federal government should establish one agency solely responsible for cryptocurrency regulation to promote innovation in the industry).
132 *Id.* at 1027.
133 Barrack, *supra* note 127, at 480, 481.
134 *Id.* at 481.
135 Werbach, *supra* note 87, at 531.
139 *See generally* House Comm. on Agric. – Republicans, *supra* note 89.
extent and limitation of the CFTC’s jurisdictional reach over cryptocurrency.\textsuperscript{140} It then establishes boundaries for how and where certain transactions involving digital commodities can occur.\textsuperscript{141} Finally, the DCEA provides for the registration and operation of digital commodity exchanges to facilitate these transactions in a manner that protects market integrity and customer assets.\textsuperscript{142}

The DCEA first establishes the boundaries of the CFTC’s regulation over cryptocurrency.\textsuperscript{143} The act begins by defining a digital commodity as personal property that is tangible, is freely exchangeable, can be exclusively possessed, can be transferred to another person, and does not require an intermediary for transfer.\textsuperscript{144} Next, the DCEA gives the CFTC “exclusive jurisdiction over any agreement, contract, or transaction involving” the sale of these digital commodities through a registered entity in interstate commerce.\textsuperscript{145} Furthermore, the CFTC would obtain jurisdiction over agreements, contracts, or transactions involving digital commodity presales, including “any promise or right to a future” digital commodity subject to certain restrictions.\textsuperscript{146} This does not limit the regulatory authority of any state or other federal agency.\textsuperscript{147}

Further, the DCEA seeks to limit the types of transactions that can occur involving digital commodities.\textsuperscript{148} First, a person may trade in digital commodities obtained through digital commodity presales both off-exchange and on-exchange in certain situations.\textsuperscript{149} A person may trade digital commodities obtained through presales if the amount is within CFTC-established limits, or in order to receive the

\textsuperscript{140} H.R. 8373 § 2(a), (b).
\textsuperscript{141} Id. at § 2(c).
\textsuperscript{142} Id. at § 2(c)–(e).
\textsuperscript{143} Id. at § 2(a), (b).
\textsuperscript{144} Id. at § 2(a) (“The term ‘digital commodity’ means any form of fungible intangible personal property that can be exclusively possessed and transferred person to person without necessary reliance on an intermediary. The term ‘digital commodity’... does not represent any financial interest in a company, partnership, or investment vehicle.”).
\textsuperscript{145} Id. at § (2)(b).
\textsuperscript{146} Id. at § (2)(b). The act provides that the CFTC would “have exclusive jurisdiction over any agreement, contract, or transaction involving a unit of a digital commodity, or any promise or right to a future unit of a digital commodity, obtained through a digital commodity presale and subject to restrictions.” Id. The DCEA defines a digital commodity presale as “the delivery of... a digital commodity, or any promise or right to a future unit of a digital commodity, to a participant in a securities offering conducted in compliance with the Securities Act of 1933 before the listing of the digital commodity for trading on a registered digital commodity exchange.” Id. at § 2(a).
\textsuperscript{147} Id. at § (2)(b) (“Nothing in this subparagraph shall be construed to limit the power of any State or other federal regulatory agency, or to provide the Commission with jurisdiction, with respect to –(I) custodial or depository activities for a digital asset, or custodial or depository activities for any promise of right to a future digital asset, of an entity regulated by a State or another Federal regulatory agency; or (II) a securities offering or transaction.”).
\textsuperscript{148} H.R. 8373 § 2(c).
\textsuperscript{149} Id. For off-exchange transactions, a person may use a digital commodity presale to trade in digital commodity futures, if the transaction complies with the Securities Act of 1933, or to sell a digital commodity to an accredited investor. Id. For on-exchange transactions, a person can sell or exchange any digital commodity obtained through a digital commodity presale or through the previously described transaction on a registered digital commodity exchange, as long as the transaction complies with the exchange’s rules. Id. A digital commodity exchange is “a trading facility that lists for trading at least one digital commodity.” Id. at § (2)(a).
non-financial rights or services associated with them. Finally, digital commodities are not subject to any transaction restrictions if they were publicly available for trading through a licensed money transmitter prior to the act’s enactment.

The DCEA then seeks to provide guidance for registering, operating, and maintaining digital commodity exchanges. Registering as a digital commodity exchange with the CFTC is voluntary, and trading facilities can choose instead to register with states and follow their regulations. If a trading facility does choose to register with the CFTC, it must first show that it is not subject to manipulation. Once the trading facility is registered with the CFTC as a digital commodity exchange, it must follow its operational guidelines. The trading facility, however, gains certain benefits, such as leveraged trading and “reasonable discretion” in how it chooses to comply with the guidelines.

A registered digital commodity exchange must establish and enforce certain trading, trade processing, and participation rules to keep its exchange fair and protect customers. For instance, exchanges must provide “participants with impartial access to the market” and ensure they are not susceptible to manipulation. They must also monitor all trading and publish trading information in a timely fashion. Furthermore, the exchange must have procedures in place to protect customer assets, such as not comingling money and minimizing risks of financial loss or delays in receiving funds. The act, additionally, makes it unlawful for exchanges to misuse customer assets and obliges them to maintain adequate financial resources, as determined by the CFTC, to meet their obligations. Lastly, the exchanges must establish procedures “to identify and minimize sources of operational and security risks” as well as emergency, backup,
and recovery procedures, including arranging periodic testing of these procedures.\textsuperscript{162}

III. THE REGULATORY PATH THROUGH THE DCEA: A USE-BASED REGULATORY APPROACH FOR CRYPTOCURRENCY

Congress should pass similar legislation to the DCEA and create a use-based regulatory framework for cryptocurrency.\textsuperscript{163} The DCEA’s strength is its narrow scope.\textsuperscript{164} The act regulates digital assets only when used specifically as commodities, and not, for example, when used as a securities.\textsuperscript{165} Although the DCEA is imperfect, it does not try to overregulate nor does it place too many restrictions on the industry.\textsuperscript{166} Instead, the act simply attempts to address the market risks when cryptocurrency is used as a commodity.\textsuperscript{167} If Congress passes similar legislation for other federal agencies, it would achieve a flexible, use-based regulatory framework that would provide greater stability to the market, allow for continued innovation, and mitigate criminal activity and risks to consumers.\textsuperscript{168}

Section A of this Part examines the strengths of the DCEA and how it manages to mitigate some of the risks posed to the market when cryptocurrency is used as a commodity.\textsuperscript{169} Section B of this Part discusses where the DCEA falls short on providing clarity to the market and providing consumer protection mechanisms.\textsuperscript{170} Finally, Section C of this Part argues that passing legislation with similar strengths as the DCEA will benefit the cryptocurrency market and is consistent with how Congress has regulated other innovative technologies.\textsuperscript{171}

\textit{A. Strengths of the DCEA: Enhanced Consumer Protection and the Potential for Great Market Stability}

\textsuperscript{162} \textit{Id.}
\textsuperscript{165} H.R. 8373 § 2(a), (b).
\textsuperscript{166} \textit{Id.} at § 2.
\textsuperscript{167} H.R. 8373 § 2(e).
\textsuperscript{168} \textit{Id.; see also} Kuegler, supra note 164, at 1015 (arguing that businesses could more easily comply with regulations if Congress passed legislation that gives federal agencies explicit control over cryptocurrency); Tu & Meredith, supra note 163, at 345, 346 (arguing for an interagency regulatory framework for cryptocurrencies that promotes communication and collaboration).
\textsuperscript{169} See discussion \textit{infra} notes 172–195 and accompanying text.
\textsuperscript{170} See discussion \textit{infra} notes 196–225 and accompanying text.
\textsuperscript{171} See discussion \textit{infra} notes 226–260 and accompanying text.
The DCEA establishes the outer boundaries of the CFTC’s jurisdiction over the cryptocurrency market and follows a policy objective of consumer protection by setting standards for digital commodity exchanges that mitigate risks in the marketplace. This approach would ultimately foster the growth of the digital commodities market by creating more trust in the system.

The strongest aspect of the DCEA is its attempt to regulate cryptocurrency based on its use. The act clearly defines a digital commodity and when a digital asset is used as a digital commodity, allowing cryptocurrency companies to know when their digital asset will fall under the CFTC’s jurisdiction. Furthermore, the DCEA explicitly states that it does not restrict the regulatory authority of any other federal or state agency. These clear jurisdictional boundaries help guide CFTC regulation and allow the CFTC to continue working in concert with other federal agencies. This approach creates more flexibility for the system by capturing only cryptocurrencies that exchanges and consumers use in a certain manner. As a result, cryptocurrency companies would know when they do need and do not need to comply with the CFTC’s regulations, mitigating fears of regulatory overreach.

Another strength of the DCEA is that it uses the digital exchange as a medium to protect against criminal activity, consumer abuse, and asset mismanagement. One of the challenges for regulators is that cryptocurrencies are not legal entities. The third-party intermediaries that facilitate cryptocurrency

172 H.R. 8373 § 2(a), (b), (c); see Kuegler, supra note 164, at 1015 (arguing that legislation which provides federal agencies with jurisdiction over cryptocurrency will help the industry grow); Tu & Meredith, supra note 163, at 327 (arguing that a regulatory regime should focus on mitigating the risks posed by the technology).
173 See Werbach, supra note 163, at 528, 532 (implementing government regulations allowed for the widespread adoption of the internet because it resolved economic inefficiencies and created trust in the technology).
174 H.R. 8373 § 2(a); see Werbach, supra note 163, at 540 (noting that the government successfully created regulations for the internet through acts such as the Communications Decency Act).
175 H.R. 8373 § 2(a), (c); see Kuegler, supra note 164, at 1015 (arguing that legislation granting federal agencies specific control over cryptocurrency would improve the current regulatory framework).
176 H.R. 8373 § 2(b).
177 H.R. 8373 § 2(b); see Kuegler, supra note 164, at 1015 (arguing that if Congress explicitly defined the jurisdictional boundaries held by federal agencies over cryptocurrency, the agencies could work together to create a better regulatory framework); Tu & Meredith, supra note 163, at 345, 346 (arguing that communication and collaboration between federal agencies is key to efficiently regulating cryptocurrency and that these agencies should focus on mitigating the risks associated with cryptocurrencies).
178 See Tu & Meredith, supra note 163, at 345 (arguing that regulating cryptocurrency is consistent with the policy objective for regulating currency, payments, financial services, banking, and investment law).
179 See Kuegler, supra note 164, at 1015 (arguing that explicitly defining federal agencies’ roles will make cryptocurrency regulation more effective).
180 H.R. 8373 § 2(e); see Tu & Meredith, supra note 163, at 329 (arguing that agencies should focus on intermediaries that facilitate transactions, such as exchanges, when creating regulations because they are easier to hold to compliance standards than cryptocurrency).
181 Tu & Meredith, supra note 163, at 332.
transaction, however, are legal entities. As a result, regulators can more easily restrict them.

The DCEA uses restrictions to provide reasonable measures that mitigate the inherent risks in the cryptocurrency market. For example, the act requires digital commodity exchanges to adopt system safeguards to protect customers’ assets against malicious outside actors such as hackers. To guard against fraud, the act prohibits the sale of digital commodities that are susceptible to market manipulation and makes it illegal for digital exchanges to misuse customer funds. Additionally, the DCEA requires digital commodity exchanges to establish mechanisms that will identify violations of the act and create procedures that protect customer assets in a manner that mitigates risk. Lastly, it protects consumers against losses from mismanagement by prohibiting the comingling of funds and requiring digital commodity exchanges to maintain adequate levels of capitalization.

The act accomplishes this goal of consumer protection by using relatively broad language. This approach sets objectives for both the CFTC and digital commodity exchanges while allowing both parties to determine the best individual methods for achieving them. Combined, these mechanisms provide clear sets of guidelines for companies to follow, reducing the level of risk in the cryptocurrency marketplace and allowing it to grow.

This regulatory approach should generally allow the market for digital commodities to prosper. The clear boundaries of the CFTC’s jurisdiction and the DCEA’s risk mitigation goals would bring stability to the market. Cryptocurrency companies could then more easily comply with the law and grow their businesses because they would understand which laws and regulations they

---

182 Id.
183 Id. at 329.
184 H.R. 8373 § 2(e). See Tu & Meredith, supra note 163, at 332, 327 (arguing that regulators should focus on mitigating the risks associated with technologies).
185 H.R. 8373 § 2(e).
186 Id.
187 Id.
188 Id.
189 Id.
190 H.R. 8373 § 2(e); see Tu & Meredith, supra note 163, at 347 (arguing that setting policy goals is important to creating a coherent regulatory framework).
191 H.R. 8373 § 2(e); see Tu & Meredith, supra note 163, at 337–38 (noting that without regulation Bitcoin has experienced extreme and volatile price corrections resembling speculative bubbles); see, e.g., Werbach, supra note 163, at 528, 532 (arguing that government regulation mitigated initial risks associated with the internet and allowed for its widespread adoption).
192 See Werbach, supra note 163, at 528, 532 (noting that society did not accept the internet until the government passed regulations fixing its economic inefficiencies).
193 H.R. 8373 § 2(a), (b), (e); see Tu & Meredith, supra note 163, at 327 (arguing that government should focus on risk mitigation when creating regulatory frameworks); Kuegler, supra note 164, at 1015 (discussing the need for federal agencies to have explicit guidance from legislation to establish a strong regulatory framework for cryptocurrency).
need to follow. The digital commodities market, as a result, could flourish by continuing to grow and innovate.

B. The DCEA’s Missed Opportunities: Lack of Clarity and Consumer Education

The DCEA, however, missed two opportunities to bring more stability and certainty to the digital commodities market. First, the act has vague, unclear language on the obligations of digital commodity exchanges during the transition to the new regulatory regime under the DCEA. Secondly, the DCEA failed to provide a mechanism or policy objective to narrow the literacy gap between consumers and companies regarding digital commodities. If passed, the DCEA’s ambiguity on how digital commodity exchanges should transition into the new regulatory regime may create uncertainty that harms the market and reduces the act’s effectiveness. Congressman Conaway stated that trading facilities could opt in to the DCEA’s registration framework or continue to operate under state licenses, but the bill’s language does not make this explicitly clear. It states that “any trading facility . . . may register with” the CFTC. The bill also allows a trading facility that “has been continuously licensed as a money transmitter in at least 20 states or territories of the United States since August 1, 2019” to qualify as a registered digital commodity exchange when transitioning to the new regime. The act does not, as Congressman Conaway contends, clearly provide an either or option. The CFTC may choose to enforce it in this way in practice, but the unclear language may initially confuse companies looking to operate digital commodity exchanges in interstate commerce.

Additionally, the DCEA missed an opportunity to better educate consumers on the digital commodities offered through the digital exchanges, allowing them to

---

194 Werbach, supra note 163, at 528, 532 (discussing how government regulation of the internet addressed market inefficiencies leading to its acceptance by the public).
195 H.R. 8373. See Werbach, supra note 163, at 528, 532 (arguing that government regulation allowed for the widespread adoption and development of the internet by creating trust in the technology).
197 H.R. 8373 § 2(e).
198 Id. See Makonnen, supra note 196, at 580 (arguing that a lack of literacy in cryptocurrency technology increases the risks to consumers).
199 H.R. 8373 § 2(e). See John W. Bagby et al., An Emerging Political Economy of the Blockchain: Enhancing Regulatory Opportunities, 88 U. Mo. Kan. City L. Rev. 419, 422 (2019) (discussing how bad regulation may harm the cryptocurrency market by creating negative externalities); Kuegler, supra note 164, at 1015 (discussing the need for federal agencies to have explicit guidance from legislation to establish a strong regulatory framework for cryptocurrency).
201 H.R. 8373 § 2(e) (emphasis added).
202 H.R. 8373 § 2(e).
203 Id.; House Comm. on Agric. – Republicans, supra note 200, at 2.
204 See Bagby, supra note 199, at 422 (discussing how bad regulation may harm the cryptocurrency market by creating negative externalities).
invest with more awareness of the potential risks.205 The act only requires digital commodity exchanges to publicly disclose trading data to consumers.206 It does not require them to provide any information about the underlying digital commodity itself.207 Even with full financial disclosures, most investors probably do not fully understand the technology in which they are investing.208 The technology is new, complex, and lacks consistently clear investment guidance from the government on each individual digital commodity.209

Having either the digital exchange or the CFTC provide basic information on the underlying digital commodity, though, would follow the traditional regulatory approach: more informed consumers make better decisions.210 Regulators generally follow the theory that market efficiency depends on information distribution and consider company disclosures as one of the best methods at their disposal to reduce investor risk.211 Disclosures educate investors on the risk involved with the asset, allow consumers to choose whether to take the risk, and limit government intrusion in the marketplace.212

This approach is common amongst financial regulators and regulators of cryptocurrency.213 For example, the SEC responded to Enron and other corporate and accounting scandals by proposing new disclosure requirements for companies.214 In 2014, the Consumer Financial Protection Bureau posted a warning on their website to advise consumers on the various risks posed by cryptocurrencies.215 Similarly, the Federal Trade Commission has offered workshops to educate consumers on cryptocurrency and identifying scams.216

Policymakers have also adopted similar approaches for other technology to reduce the risks to consumers.217 When technological restrictions failed to improve

205 H.R. 8373; see Werbach, supra note 163, at 519 (discussing how investors’ lack of understanding of blockchain technology leaves them open to scams).
206 H.R. 8373 § 2(e).
207 H.R. 8373 § 2(e).
208 Werbach, supra note 163, at 519.
209 Id.
210 See Susanna Kim Ripken, Paternalism and Securities Regulation, 21 STAN. J.L. BUS. & FIN. 1, 2 (2015) (discussing how securities law and the SEC require market investors to make material information available to allow investors to make more informed decisions).
211 Ronald J. Gilson & Reinier H. Kraakman, The Mechanisms of Market Efficiency, 70 VA. L. REV. 549, 592 (1984); Ripken, supra note 210, at 2 (noting that the Supreme Court has prevented the SEC from adopting more substantive regulations beyond disclosures that oversee a corporation’s governance practices).
212 Ripken, supra note 210, at 2; see id. (discussing how securities law and the SEC require market investors to make material information available to allow investors to make more informed decisions); see also Troy A. Paredes, Blinded by The Light: Information Overload and Its Consequences for Securities Regulation, 81 WASH. U. L.Q. 417, 419 (2003) (noting that studies have found that overloading consumers with information causes them to make worse decisions).
213 See, e.g., Paredes, supra note 212, at 418.
214 Paredes, supra note 212, at 418.
privacy, security, and safety risks from the internet of things (IoT) and wearable technologies, the Obama Administration decided to educate the public instead, and to help them make more informed decisions when using the internet and related technology.\textsuperscript{218} The program sought to inform consumers of the risks involved in using IoT and wearable technology and the proper and improper uses of the technology.\textsuperscript{219} The Administration found this method easier to implement than placing additional technological or legal restraints on companies.\textsuperscript{220} Requiring either the CFTC or the company itself to publicly provide basic information about the underlying digital commodity would similarly help consumers develop this literacy.\textsuperscript{221} As a result, they could make better informed, less risky decisions in a highly volatile market.\textsuperscript{222}

Although the CFTC could theoretically resolve both these issues, the DCEA nevertheless missed an opportunity to mitigate risks to the market at the start.\textsuperscript{223} Commentators and companies who are wary of government regulation of cryptocurrency may see a haphazard transition as a confirmation of their fears, which could lead to a chilling effect on any future legislation.\textsuperscript{224} Furthermore, the DCEA’s consumer protections mechanisms may have less of an effect if consumers still continue to make risky investments in digital commodities because they do not fully understand the technology in which they are investing.\textsuperscript{225}

\textbf{C. Using the DCEA as a Guide to Create a Coherent Regulatory Framework for Cryptocurrency}

Ultimately, Congress would need to pass similar legislation that regulates cryptocurrency’s use for other federal agencies to provide a coherent legal framework that makes the DCEA effective long term.\textsuperscript{226} Without clear guidelines for the SEC, FinCEN, and other federal agencies, companies and consumers would

\begin{enumerate}
\item Id. at 86.
\item Thierer, supra note 217, at 86.
\item Id. at 84.
\item See Makonnen, supra note 196, at 580 (arguing that literacy in cryptocurrency will help reduce risks to consumers).
\item See Tu & Meredith, supra note 163, at 337–38 (noting the extreme volatility of the Bitcoin market and its resemblance to speculative bubbles); Makonnen, supra note 196, at 580 (arguing that consumers will face less risks if they are more literate in the technology underlying cryptocurrency); Werbach, supra note 163, at 519 (discussing how investors have greater exposure to scams because of their lack of understanding of blockchain technology); Chu, supra note 110, at 2338, 2340 (2018) (discussing the lack of transparency in how cryptocurrency platforms manage customer assets, even though they have the same custodial relationship with customers as brokers).
\item H.R. 8373; see Tu & Meredith, supra note 163, at 327 (arguing that regulators should focus on mitigating risk when developing regulation).
\item H.R. 8373 § 2(c); see, e.g., Werbach, supra note 163, at 521–22.
\item H.R. 8373 § 2(e); see Makonnen, supra note 196, at 580 (arguing that consumers will face less risks if they increase their literacy in cryptocurrency).
\item H.R. 8373. See Kuegler, supra note 164, at 1015 (noting that federal agencies need definitive guidance from Congress to effectively regulate); see also Werbach, supra note 163, at 532 (noting the jurisdictions trying to attract cryptocurrency companies do not engage in races to the bottom for regulation).
\end{enumerate}
still operate with a high level of uncertainty. Companies will still be unclear about industry regulations, and consumers will continue to lack protection in the cryptocurrency market that operates outside the CFTC’s control. Congress needs to update the current piecemeal legal structure for cryptocurrency either by passing the DCEA and similar legislation for other federal agencies or by passing omnibus legislation that provides explicit jurisdiction and guidelines for federal agencies.

Relying on the current federal regulatory agencies to regulate cryptocurrency is probably the best method to balance the competing interests of consumer protection and innovation because this method would regulate cryptocurrency based on its use. Similar to the internet in the nineties, the cryptocurrency market is reaching the point where it needs government regulation to operate efficiently. The cryptocurrency market requires the government’s support to both prevent and prosecute hackers and fraudsters and to establish baseline best practices that allow legitimate cryptocurrency businesses to obtain consumer trust. Congress has successfully created these legal frameworks for the internet and other new and evolving technologies based on their use.

The internet in the 1990s serves as the best example of a legal framework based on the technology’s use. Similar to blockchain and cryptocurrency, commentators thought that the internet undermined regulation through decentralization. They believed the internet could operate completely outside of legal restrictions because the government could not possess it nor control it. Like cryptocurrency, however, the internet served just as much as a platform for bad actors as it did an opportunity for advancing society. Eventually, companies called for governments to curtail some of this bad behavior.

Hearing the call, Congress decided to update old legislation and pass new laws that regulated the internet based on how companies and consumers interacted

227 Kuegler, supra note 164, at 1015 (arguing that without specific legislation, federal agencies lack proper guidance for regulating cryptocurrency).
228 See Kuegler, supra note 164, at 1025 (discussing confusion around SEC guidance for cryptocurrency).
230 Bagby, supra note 199, at 449; Kuegler, supra note 164, at 1009 (arguing that because federal agencies have a higher rate of policy making than Congress, they are better suited to handle quickly changing technology).
231 See Werbach, supra note 163, at 528 (noting that, in the nineties, the federal government brought an antitrust suit against Microsoft to prevent it from using its monopoly power to push out internet startups).
233 Werbach, supra note 163, at 529.
234 Werbach, supra note 163, at 504.
235 Id. at 520.
236 Id.
237 Id. at 528.
238 See id. (discussing how commentators started to call for the government to enforce network neutrality and privacy protections to help society trust the internet).
with it.\textsuperscript{239} Although the internet is decentralized, online platforms and service providers exist within traditional jurisdictional boundaries.\textsuperscript{240} This structure allowed Congress to avoid creating a new regulatory agency or enacting some broad sweeping law.\textsuperscript{241} Importantly, it also did not simply standby and hope the free market would eventually solve all the internet’s issues.\textsuperscript{242} Instead, Congress took action to address where the market was falling short in fostering a fair and efficient business practices.\textsuperscript{243}

For example, Section 230 of the Communications Decency Act (CDA) provided safe harbors that allowed internet services providers and social media platforms to flourish.\textsuperscript{244} These safe harbors shielded websites from liability against users who posted content on their platforms.\textsuperscript{245} Companies, such as Facebook or Twitter, consequently, are not liable if someone posts defamatory speech on their platforms.\textsuperscript{246} Commentators largely attribute these Section 230 safe harbors to the success of the internet because they allowed these internet platforms to develop without the fear of burdensome government regulation.\textsuperscript{247}

Similarly, the Digital Millennium Copyright Act (DMCA) provided important copyright safe harbors for internet service providers that allowed companies like Google and YouTube to flourish.\textsuperscript{248} The act did not take away rights for copyright owners.\textsuperscript{249} Instead, similar to the CDA, it protected internet service providers from liability if users posted or transmitted copyrighted material as long as the internet service providers established and implemented a repeat infringer policy and a notice and takedown process.\textsuperscript{250} If the internet service provider does not comply with this requirement, then it loses its liability shield.\textsuperscript{251} This system eventually allowed the DMCA to create a more competitive marketplace by providing stability and direction for the industry, which allowed companies like Google and YouTube to flourish.\textsuperscript{252}

\textsuperscript{240} Werbach, supra note 163, at 521.
\textsuperscript{241} Id.
\textsuperscript{242} Id. at 528; Minor, supra note 239, at 1167; see, e.g., 17 U.S.C. § 512; 47 U.S.C. § 230.
\textsuperscript{243} Werbach, supra note 163, at 528; Minor, supra note 239, at 1167; see, e.g., 17 U.S.C. § 512; 47 U.S.C. § 230.
\textsuperscript{244} 47 U.S.C. § 230; Werbach, supra note 163, at 540.
\textsuperscript{245} 47 U.S.C. § 230(c)(9), (d); Werbach, supra note 163, at 540.
\textsuperscript{247} 47 U.S.C. § 230; Werbach, supra note 163, at 540; Khanna, supra note 246.
\textsuperscript{248} 17 U.S.C. § 512; Minor, supra note 239, at 1154.
\textsuperscript{249} 17 U.S.C. § 512.
\textsuperscript{250} Id. § 512(c)(1)(C), (i)(1)(A). Internet service providers must adopt, implement, and inform subscribers of termination policy for repeat infringers. Id. § 512(i)(1)(A). They also must adopt standard technical measures used by copyright owners to identify and protect copyrighted works and respond to copyright owners request for the removal of material. Id. § 512(c)(1)(C), (i)(1)(B).
\textsuperscript{251} 17 U.S.C. § 512(i).
\textsuperscript{252} 17 U.S.C. § 512; Minor, supra note 239, at 1154.
The current cryptocurrency market is similar to where the internet was in the nineties, and, just like the internet, regulations on cryptocurrency use will not stifle innovation.\textsuperscript{253} Internet service providers and other technology companies did not seek to operate from the least regulated jurisdictions.\textsuperscript{254} They chose jurisdictions such as Silicon Valley where the developers, customers, and regulations that best served their needs.\textsuperscript{255} A well thought out regulatory framework that seeks to regulate digital assets by use can do the same for the cryptocurrency market.\textsuperscript{256}

Passing similar legislation to the DCEA would allow Congress to fill the various gaps in the current regulatory framework for cryptocurrency while maintaining a competitive environment for the industry to flourish.\textsuperscript{257} Federal agencies such as the CFTC, SEC, and FinCEN, are well suited to regulate the cryptocurrency market because of how quickly they can adapt through the rulemaking process and their expertise in financial instruments.\textsuperscript{258} If Congress provided them with similar guidance as it did with the internet in the 1990s, the agencies could establish a cohesive regulatory framework that can adapt to the various risks and opportunities the cryptocurrency market presents.\textsuperscript{259} Consequently, Congress should enact acts like the DCEA to create a regulatory framework that brings stability to the cryptocurrency market, allowing it to thrive.\textsuperscript{260}

\textbf{CONCLUSION}

The DCEA is not perfect, but neither is any legislation Congress will adopt. Congress needs to create an effective legal framework for regulating the cryptocurrency market based on investor and user use. To accomplish this task, though, Congress needs to enact more legislation similar to the DCEA that provides federal agencies with explicit jurisdiction and guidance for regulating the cryptocurrency market. This approach would enable Congress to properly balance the need to prevent criminal activity and protect consumers against the desire to promote the development of the cryptocurrency industry.

\textsuperscript{253} See Werbach, supra note 163, at 528, 532 (discussing how implementing government regulations allowed for the continued development of the internet because it resolved economic problems and created trust in the technology).
\textsuperscript{254} Id. at 528, 532.
\textsuperscript{255} Id.
\textsuperscript{256} See Minor, supra note 239, at 1154 (noting how both YouTube and Google benefited from the regulatory environment partially created by the Digital Millennium Copyright Act).
\textsuperscript{257} See Werbach, supra note 163, at 528, 532 (discussing how government regulations resolved economic inefficiencies and risks associated with the internet).
\textsuperscript{258} Bagby, supra note 199, at 449; Kuegler, supra note 164, at 1009.
\textsuperscript{259} Werbach, supra note 163, at 528–29, 529 (comparing blockchain to the internet and citing the internet as a positive model of the government working with nascent industries to create effective regulation).
\textsuperscript{260} See H.R. 8373; Werbach, supra note 163, at 528, 532 (arguing that government regulation created trust in the internet, which ultimately allowed it to continue to develop and thrive).