Regulating Blockchain? An Ex-Post Regulatory Impact Assessment of the U.S. Blockchain Regulatory Regime

Jiaying Christine Jiang *

ABSTRACT

Blockchain technology has significant impacts on financial services. U.S. regulation regards blockchain technology as a type of financial technology when it provides financial-related products or services, which belong to one of the most heavily regulated sectors of the economy. However, blockchain technology and its applications constantly present novel problems that require regulatory responses. Regulators, academics, and the business world have been arguing whether new regulations are needed to target blockchain technology and its applications, either by providing a facilitative structure (recognition) or restrictive regulatory provisions (licensing, reporting, and anti-money laundering). To properly understand whether new regulations are needed, a prerequisite (as well as the missing step) is to evaluate how the existing regulatory regime works. This article fills the gap by relaying a regulatory impact assessment of the existing blockchain regulatory regime.

This article first summarizes the overall blockchain regulatory landscape at the federal level and then contains an ex-post regulatory impact assessment. The regulatory landscape consists of actions such as interpreting existing regulations; issuing official guidance, statements, or alerts; piloting blockchain-related initiatives; and enforcement. The assessment consists of three major steps. The first is to explain the problems before taking regulatory action. The second is to identify the objectives of the existing regulatory regime for blockchain and its applications, and the third is to determine whether these objectives have been fulfilled. From the analysis, this article identifies three major problems: (1) fraud and scams in the cryptocurrency market, (2) law enforcement difficulties, and (3) immature blockchain products and services. In responding to these problems, existing regulatory actions have four objectives: (1) maintaining a fair and efficient market, (2) consumer and investor protection, (3) criminal enforcement, and (4) technology innovation. These four objectives are major indicators used to assess regulatory impacts and whether objectives have been satisfied.

*Jiaying Christine Jiang, S.J.D., Hauser Global Fellow at New York University School of Law

Table of Contents

I. REGULATORY LANDSCAPE 5
A. THE SECURITIES EXCHANGE COMMISSION 6
1. The DAO Actions 6
2. FinHub 8
3. Other SEC press releases, investor alerts, investor bulletins, and other SEC Commissioners' statements 9
B. THE COMMODITY FUTURES TRADING COMMISSION 10
1. CFTC's Smart Contract 11
2. CFTC and Bitcoin 11
3. Other CFTC Actions and Commissioner Speeches 12
C. THE DEPARTMENT OF TREASURY'S FINANCIAL CRIMES ENFORCEMENT NETWORK 13
D. THE CONSUMER FINANCIAL PROTECTION BUREAU 15
E. FEDERAL TRADE COMMISSION 15
F. THE INTERNAL REVENUE SERVICE 16
G. FEDERAL BUREAU OF INVESTIGATION AND THE DEPARTMENT OF JUSTICE'S CRIMINAL DIVISION 17
II. EX-POST REGULATORY IMPACT ASSESSMENT 18
A. WHAT WERE THE PROBLEMS BEFORE ANY REGULATORY ACTION WAS TAKEN? 18
1. Fraud and Scams in the Cryptocurrency Market 19
2. Law Enforcement Difficulties 22
3. Immature Blockchain Products and Services 23
B. WHAT ARE THE OBJECTIVES OF THE EXISTING BLOCKCHAIN REGULATORY REGIME? 25
1. Maintaining a Fair and Efficient Market 26
2. Consumer and Investor Protection 28
3. Criminal Enforcement 30
4. Technology Innovation 32
C. HAVE THESE OBJECTIVES BEEN FULFILLED? 35
1. Impacts on the Market in General 35
2. Impacts on Investor and Consumer Protection 38
3. Impacts on Criminal Enforcement 40
4. Impacts on Technology Innovation 44
a. Infrastructure for Cross-border Transactions 45
b. New Mechanism for Capital Formation 47
c. Tokenized Assets as a Class 51
III. CONCLUSION 53

INTRODUCTION

Blockchain technology, also known as distributed ledger technology (DLT), or blockchain, is a distributed database system. Supported by its consensus mechanism and cryptography, blockchain technology can provide tamper-proof, traceable, transparent, and secured data. In finance, blockchain can facilitate the delivery of increased efficiency, reduced loss and fraud, improved customer experience, and the higher availability of capital. [1] Specifically, its distributed databases are designed to avoid reconciliations by eliminating the traditional centralized system. Immutable records that are visible to all participants afford greater transparency and enhance data accuracy and security. Using blockchain to share information with clients and vendors may allow companies to expedite customer service and even identify new markets.[2] According to a Klynveld Peat Marwick Goerdeler (KPMG) analysis, blockchain technology will reduce capital consumption by means of the quicker settlement of trades, straight-through processing, and freed-up capital flows.[3]

Meanwhile, blockchain technology and its applications present novel problems that require regulatory responses. This urgent need of regulatory responses places regulators in a dilemma because legal solutions cannot always keep up with technology development. Regulators, academics, and the business world have been arguing whether new regulations are needed to target blockchain technology and its applications, either by providing a facilitative structure (recognition) or restrictive regulatory provisions (licensing, reporting, and anti-money laundering).

However, to properly understand whether new regulations are needed, a prerequisite is to evaluate how the existing regulatory regime works. An ex-post assessment of the existing regulatory regime tells regulators how well or badly they are doing, whether desired outcomes have been achieved, what the problems with the existing policies and regulations are, and what is needed to improve future legislation. A systematic examination of the impacts of existing regulatory regime also contributes to good governance and reforms.

To assess the impacts of the existing regulatory regime, the framework this article uses is the regulatory impact assessment (RIA). The Cabinet Office of the UK defines RIA as "a tool which informs policy decisions. It is an assessment of the impact of policy options in terms of the costs, benefits, and risks of a proposal."[4] The European Commission, in its Impact Assessment Guidelines, defines RIA as "a set

---

1 Tony Alejo, *Blockchain and the Future of Finance* (2018), https://advisory.kpmg.us/articles/2018/blockchain-future-finance.html. Subject: Finance and accounting

2 *Id.*

3 *Id.*

4 UK Cabinet Office, *Better Policy Making: A Guide to Regulatory Impact Assessment*, http://www.dei.gov.ba/bih_i_eu/RIA_u_BiH/default.aspx?id=6595&langTag=bs-BA (last visited Feb. 16, 2019)

of logical steps to be followed when you prepare policy proposals. [5] It is a process that prepares evidence for political decision-makers on the advantages and disadvantages of possible policy options by assessing their potential impacts."[6] The Cabinet Office of the UK and European Commission seem to emphasize RIA as a critical tool for assessing policy proposals, since they use RIA before any policy or regulation is adopted or comes into effect.

However, this article argues that the RIA is also an equally useful tool to assess the actual results of policy or regulation after adoption. Colin Kirkpatrick and David Parker have a more accurate definition of RIA for the purpose of this article: "RIA is a method of policy analysis, which is intended to assist policymakers in the design, implementation, and monitoring of improvements to regulatory systems, by providing a methodology for assessing the likely consequences of the proposed regulation and the actual consequences of existing regulations."[7]

The framework of RIA involves both ex-post evaluation on existing policies and regulations and ex-ante estimation for proposed policies and regulations. This article concentrates solely on the first part, presenting an ex-post assessment of existing blockchain regulation. The retrospective assessment consists of three questions: (1) What were the problems before any regulatory action was taken? (2) What are the objectives of the existing regulatory regime? (3) Have these objectives been fulfilled?

This ex-post RIA follows a logical order. Understanding problems in the absence of the regulatory regime is the first step for a successful RIA. A clear identification of problems allows evaluators to track root causes, set appropriate objectives, identify options to address the problems, and assess whether these problems have been solved in the end. Second, policy objectives are the intended goals of government intervention.[8] Clear policy objectives help establish a course of action and allow for identification and comparison of policy options. Third, assessing if objectives have been fulfilled helps regulators understand the extent to which a regulation is achieving its objectives, and whether the implementation is "on track." This is a preliminary and necessary step to support the next steps of rulemaking, such as changing certain rules based on the impact assessed or continuing enforcement of

---

5 European Commission, *Impact Assessment Guidelines*, http://ec.europa.eu/smart-regulation/impact/commission_guidelines/docs/iag_2009_en.pdf (last visited Mar. 30, 2019). Subject: Law

6 *Id.*

7 COLIN KIRKPATRICK AND DAVID PARKER, REGULATORY IMPACT ASSESSMENT TOWARDS BETTER REGULATION? (2008).

8 The European Commission's RIA system claims that objectives should be "SMART" – specific, measurable, achievable, realistic and time-dependent. Specifically, specific objectives should be sufficiently precise and concrete, and not be open to varying interpretations. Measurable objectives should be measured as to whether the objectives have been achieved, and the measurement can be quantified or based on a combination of description and scoring scales. Achievable objectives have goals that can be achieved through releasable efforts if the regulation requires actions by regulated groups. Realistic objectives should consist of a useful and meaningful target. Time-dependent objectives should achieve goals within a certain amount of time.

a certain rule to maximize its positive impacts.

Unlike the traditional framework of RIA that specifically focuses on policies or regulations issued by government agencies, this article takes a broader angle by looking at regulatory actions taken by regulatory agencies because U.S. regulators have not yet issued new policies or regulations specifically for blockchain implementation. Regulators regard blockchain technology as a type of financial technology when blockchain provides financial-related products or services, and regulatory agencies adapt existing regulatory frameworks for blockchain technology and its applications by interpreting existing requirements to yield guidance and enforcement actions. Therefore, interpretations of existing regulations, official guidance or statements, enforcement actions, and some innovative initiatives as regulatory actions are the focus of the ex-post RIA. This ex-post RIA studies the impacts of these regulatory actions instead of specific policies or regulations.

This article proceeds as follows. Part I summarizes the overall blockchain regulatory landscape at the federal level. Part II presents an ex-post RIA consisting of three steps; it begins by identifying problems in the absence of regulatory actions. This article singles out three of the most salient problems in the blockchain space— fraud and scams in the cryptocurrency market, law enforcement difficulties, and poor quality of early-stage blockchain products and services. The second step is to identify the objectives of the existing regulatory regime in terms of blockchain technology and its applications. Understanding regulatory objectives requires consideration of the missions of regulatory agencies and the novel nature of blockchain implementation in the financial market. Objectives thus consists of maintaining a fair and efficient market, consumer and investor protection, criminal enforcement, and technology innovation. These four objectives then are used as primary indicators, which could provide a broad outline for possible monitoring and evaluation arrangements, to examine if these objectives have been fulfilled, which is the last step of RIA.

I. REGULATORY LANDSCAPE

The overall blockchain regulatory landscape covers actions by the federal regulatory agencies (state-level regulations fall outside the scope), including but not limited to, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Department of Treasury's Financial Crimes Enforcement Network, (FinCEN), the Consumer Financial Protection Bureau (CFPB), the Federal Trade Commission (FTC), the Internal Revenue Service (IRS), the DOJ's Criminal Division, and the Federal Bureau of Investigation (FBI). These regulatory agencies oversee blockchain-related activities within their respective jurisdictions. They have been interpreting existing regulations, publishing official guidance, piloting relevant initiatives, and taking enforcement actions to exercise its regulatory power in the blockchain space. In the sections below, each of these regulatory bodies are discussed through the framework of their missions and authorities, as well as their current positions, outlooks, guidance, and actions

pertaining to blockchain technology and its applications.

A. The Securities Exchange Commission

The primary role of the SEC is to enforce federal security laws and regulate a significant segment of the securities industry, comprising of, in part, the U.S. options market and stock exchanges. In terms of blockchain technology, most of the SEC's discussions initially centered on cryptocurrencies and ICOs. Releasing the report on The DAO investigation represented the SEC's first action in the cryptocurrency field. In addition to its continuous attention in this field, the SEC has become increasingly interested in the evolution of blockchain technology. As blockchain technology may be a type of financial technology used for capital formation that is relevant to investor interfaces, the SEC then actively engages with innovators, developers, and entrepreneurs to understand and react well to this new emerging technology. For example, the SEC has launched its Strategic Hub for Innovation and Financial Technology (FinHub), and the SEC commissioners actually participate in various forums to exchange ideas with the potential regulated groups.

1. The DAO Actions

The SEC issued a Report of Investigation for The DAO, an independent organization that functioned virtually by using blockchain technology or a distributed ledger.[9] Interested persons could participate in or contribute to The DAO as investors by buying tokens using virtual currency. These investors could then sell their tokens on Web-based secondary market platforms in exchange for virtual currency or hold these tokens as an investment with certain voting and ownership rights. The SEC determined these tokens, otherwise referred to as a coin offering, were considered securities under the Supreme Court ruling in SEC v. W.J. Howey Co. In this context, securities are recognized as an investment contract under the federal securities laws. The report supported that the identification of an ICO as a security is dependent on surrounding information, which include the financial facts behind the exchange. [10]

The precedent of this decision, SEC v. W.J. Howey Co., is a 1946 Supreme Court ruling that supported the idea that an investment contract was a land, sales, and service contract under the Securities Act of 1933, and marketing and efforts conducted in to support this investment was a violation of the act. The ruling of this case led to the development of the Howey Test, which is a way to identify whether a security is considered an investment contract under the act. The Howey Test is defined as an agreement, operation, or plan in which a person invests in a shared effort and is provided with information that suggests that he or she will profit from

---

9 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, 18.

10 U.S. Securities and Exchange Commission, Public Statement by the Divisions of Corporate Finance and Enforcement on the Report of Investigation on The DAO, 2017

the work of an organizer or another third party.[11]

The Howey case is of particular interest because there are various ways to apply it to virtual assets, and several components of how to identify whether a digital asset constitutes as a security. First, there must be an investment component. An asset must be sold or there must be an offer made for the asset, which is bought or obtained in exchange for something of value, such as money or another virtual asset. Second, a common initiative must be identified as a separate component of an investment agreement. Third, there must be a rational expectancy of profits to be expected from the work of other people. For instance, a buyer may anticipate a certain profit from partaking in an endeavor, such as distributing goods, in hopes of benefiting from the sale of these goods.

This third component of the Howey Test has a set of factors that are of importance to note. One includes trusting in the work of other people. This fact coincides with two major questions, which probe whether the buyer is reasonably anticipated to trust in the work of an active participant and whether this work is unquestionably important or considered fundamental executive functions that impact the functioning of a company, rather than work that is more parliamentary. The stronger the presence of the entity, the heavier the potential purchaser is relying on the work of others. The second component of interest is that there must be a rational expectancy of profits. Profits may not necessarily refer to monetary value but may include something of value to those involved in the transaction. The third component is "other relevant considerations," which is when courts consider the financial authenticity of the deal.

The ruling from SEC v. W.J. Howey Co. remains relevant today and is commonly referred to in talks about cryptocurrency. One of the main points of interest is whether virtual currency, such as bitcoin, can be offered as a security, and if, over time, this can become something different from a security. According to William Hinman, director of corporate finance for the SEC, the question is: "Can a digital asset that was originally offered in a securities offering ever be later sold in a manner that does not constitute an offering of a security?" The DAO involves the selling of virtual tokens, which is typically done to fund projects. Buyers of these tokens entrust in completion of the project. While the project unfolds, the value of the tokens is thought to increase, prompting buyers to resell their tokens for a higher cost. But similar to the Supreme Court case, these tokens are thought to be sold to a larger audience, as Howey sold plots of land to businesspeople and hotel guests, rather than farmers. The purchasers of these tokens are less likely to use them virtually and may not even be aware of how to do so. But simply put, use of the Howey Test allows for the exploration of securities, or the tokens exchanged to raise funds for The DAO, according to its function, not its form. [12]

The DAO set the tone that the SEC applied longstanding securities law

---

11 U.S. Securities and Exchange Commission, Public Statement by the Divisions of Corporate Finance and Enforcement on the Report of Investigation on The DAO, 2017

12 William Hinman, Director, Corporate Division, Remarks at the Yahoo Finance All Markets Summit: Crypto, 2018.

principles to demonstrate that a particular token constituted an investment contract and therefore was a security under the federal securities laws.[13] Specifically, the SEC concluded that the token offering represented an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.[14]

In a following case, a California-based company, Munchee, Inc., sought $15 million in capital to improve an existing iPhone app centered on restaurant meal reviews and create an "ecosystem" in which Munchee and others would buy and sell goods and services using the tokens.[15] Munchee tried to structure tokens as utility tokens, and thus circumvented the SEC's supervision. However, in the course of the offering, the company and other promoters emphasized that investors could expect that efforts by the company and others would lead to an increase in value of the tokens and the company would take steps to create and support a secondary market for the tokens.[16] This case did not change the substance of "an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others." Thus, the SEC again emphasizes that merely calling a token a "utility" token or structuring it to provide some utility does not prevent the token from being a security.[17]

2. FinHub

FinHub was developed by the SEC to facilitate engagement with innovators, developers, and entrepreneurs in response to evolving financial technologies, methods of capital formation, market structures, and investor interfaces. [18] Specifically, FinHub is a virtual tool for companies looking to ensure compliance with federal laws, offering resources for them to use when developing a virtual commodity they wish to offer, sell, and resell to buyers. Rather than provide businesses with lengthy information about securities laws, FinHub is used as a quick and easily accessible research tool. With more businesses operating in both physical and virtual spaces, it is important for business owners to be aware of whether their associated processes are legal.

As part of a continuing effort to assist those seeking to comply with the U.S. federal securities laws, FinHub publish a framework to analyze whether a digital asset

---

13 Jay Clayton, *SEC.gov | Statement on Cryptocurrencies and Initial Coin Offerings* (2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11#_ftn6 . Subject: Finance and accounting

14 *Id.*

15 SEC.gov | Company Halts ICO After SEC Raises Registration Concerns, https://www.sec.gov/news/press-release/2017-227 (last visited Jan 27, 2018).

16 *Id.*

17 SEC.gov | Statement on Cryptocurrencies and Initial Coin Offerings, *supra* note 6. Subject: Law and Finance

18 *FinHub Strategic Hub for Innovation and Financial Technology*, https://www.sec.gov/finhub. Subject: Finance and accounting (last visited Jul 30, 2019).

is an investment contract and whether offers and sales of a digital assets are securities transactions.[19] The framework addresses each of the elements of the Howey Test— the investment of money, common enterprise, and reasonable expectation of profit derived from efforts of others—and specifically discusses key factors that participants should consider to reach conclusions. Although all factors are not exhaustive, they do provide guidance to assist participants engaging in the offer, sale, or distribution of a digital asset and clear some misunderstandings.[20]

3. Other SEC press releases, investor alerts, investor bulletins, and other SEC Commissioners' statements

In addition to the SEC's important actions on the investigation of The DAO and the establishment of FinHub, the SEC has responded in a variety of ways to issues arising from cryptocurrencies and blockchain technology. The SEC constantly issues investor alerts, investor bulletins, and press releases, and commissioners continuously speak at various forums to educate both private and public sectors. For example, investor alerts have been frequently educating the public about Ponzi Schemes using virtual currencies; [21] bitcoin and other virtual currency-related investments; [22] public companies making ICO-related crimes; [23] and celebrity endorsements in some investments. [24] Investor bulletins have covered ICOs and

---

19 SEC.gov | Framework for "Investment Contract" Analysis of Digital Assets, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets (last visited Jul 30, 2019). This framework represents the views of the Strategic Hub for Innovation and Financial Technology ("FinHub," the "Staff," or "we") of the Securities and Exchange Commission (the "Commission"). It is not a rule, regulation, or statement of the Commission, and the Commission has neither approved nor disapproved its content. Further, this framework does not replace or supersede existing case law, legal requirements, or statements or guidance from the Commission or
Staff. Rather, the framework provides additional guidance in the areas that the Commission or Staff has previously addressed. *See, e.g., Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Exchange Act Rel. No. 81207) (July 25, 2017) ("*The DAO Report*"); William Hinman, *Digital Asset Transactions: When Howey Met Gary (Plastic)*,
Remarks at the Yahoo Finance All Markets Summit: Crypto (June 14, 2018), available at https://www.sec.gov/news/speech/speech-hinman-061418.

20 *Id.* as stated by the SEC, this framework is intended to be instructive and is based on the staff's experiences to date and relevant law and legal precedent. It is not an exhaustive treatment of the legal and regulatory issues relevant to conducting an analysis of whether a product is a security, including an investment contract analysis with respect to digital assets generally. We expect that analysis concerning digital assets as securities may evolve over time as the digital asset market matures. Also, no one factor is necessarily dispositive as to whether or not an investment contract exists.

21 SEC Office of Investor Education and Advocacy, *Ponzi Schemes Using Virtual Currencies* (2013), https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf (last visited Jul 30, 2019).

22 Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies* (2016). 308. Subject: Finance and accounting

23 SEC.gov | Investor Alert: Public Companies Making ICO-Related Claims, , https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_icorelatedclaims (last visited Jul 30, 2019). 24 Investor Alert: Celebrity Endorsements | Investor.gov, https://www.investor.gov/introduction-

blockchain technology. [25] Press releases have been exposing suspicious ICO activities[26] or scams.[27] The SEC also hosted a Fintech forum on distributed ledger technology and digital assets to stay informed and adapt to the changing needs of market participants.[28]

SEC commissioners also express their views and concerns to the public. In a Senate Committee on Appropriations meeting in May 2019, SEC Chairman Clayton argued the significance of the agencies becoming literate in digital assets.[29] Indeed, Clayton noted that the SEC's Office of Compliance Inspections and Examinations has named "digital assets, including cryptocurrencies, coins and tokens" as high-risk investments. In addition, Clayton told the committee that the SEC has requested four new positions within the Division of Trading and Markets, which regulates major securities market participants, to help augment the agency's knowledge and capability in regard to digital asset markets. The SEC is particularly interested in market manipulation but has yet to offer any new blockchain regulation.

Commissioner Hester Peirce stated that the SEC's opportunity to rethink its approach to innovation also arises out of a decade of technological development related to blockchain and cryptocurrencies, and admitted that "blockchain-based networks offer a new way of coordinating human action that does not fit as neatly within our securities framework."[30] She keeps an open mind as to the development of blockchain technology by delaying in drawing clear lines and thus allows more freedom for the technology to come into its own.

B. The Commodity Futures Trading Commission

The CFTC is a significant overseer in the regulation of the financial market, working to protect market participants from fraud and dishonest individuals and those participants' confidence and trust in those markets. The CFTC's main purpose is to oversee the options and commodity futures markets. More recently, the CFTC is shifting its focus solely as an overseer of conventional commodity product-related

---

investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/investor-22, (2017), https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-celebrity- endorsements. Subject: Finance and accounting (last visited Jul 30, 2019).

25 SEC.gov | Investor Bulletin: Initial Coin Offerings, , https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings (last visited Jul 30, 2019).

26 SEC.gov | SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds, , https://www.sec.gov/news/press-release/2017-185-0 (last visited Jul 30, 2019).

27 SEC.gov | SEC Halts Alleged Initial Coin Offering Scam, , https://www.sec.gov/news/press-release/2018-8 (last visited Jul 30, 2019).

28 SEC.gov | SEC Hosts FinTech Forum on Distributed Ledger Technology and Digital Assets, , https://www.sec.gov/sec-hosts-fintech-forum-on-distributed-ledger-technology-and-digital-assets (last visited Jul 30, 2019).

29 SEC.gov | Testimony before the Financial Services and General Government Subcommittee of the U.S. Senate Committee on Appropriations,, https://www.sec.gov/news/testimony/testimony-financial- services-and-general-government-subcommittee-us-senate-committee (last visited Jul 30, 2019).

30 SEC.gov | Regulation: A View from Inside the Machine, , https://www.sec.gov/news/speech/peirce- regulation-view-inside-machine (last visited Feb 11, 2019).

futures and options, moving towards regulation of cryptocurrencies and blockchain. The CFTC has noted that these technological innovations will impact CFTC- regulated markets, as well as the agency itself, through artificial intelligence, algorithmic trading, machine learning, distributed ledgers, and network cartography. However, given there is not yet a monolithic federal classification for cryptocurrencies, neither the CFTC nor the SEC have uniform regulations, leading to disparate policies and standards, though both equally enforceable by both agencies. Despite this lack of consistent standards, policies, and definitions, the CFTC has demonstrated a willingness and eagerness to oversee the emerging technology.

1. CFTC's Smart Contract

In a continued effort to better prepare for the discussion caused by digital assets, the CFTC and its LabCFTC recently released its smart contracts primer. LabCFTC is an initiative developed by the CFTC to encourage responsible FinTech innovation for Americans' collective gain.[31] LabCFTC is intended to make the CFTC more comprehensible to Fintech developers and presents itself as a way to educate the CFTC about new innovations. The role of LabCFTC is to provide insight into product advancement.

The smart contracts primer is an explanation of smart contracts as encrypted computer processes that may entail components of a binding contract or implement specific conditions to an external contract.[32] Simply put, a smart contract is a set of programmed computer functions. Smart contracts allow for the terms and conditions of a contract to take effect at specific times or based on whether an event does or does not occur. This may include wide-sweeping variables, from product delivery to a change in the cost of similar product, to the current weather situation. The report also laid out three main attributes of a smart contract: it can authenticate (counter) party identities, the ownership of assets, and claims of right; it can access or refer to outside information or data to trigger action(s); and it can automate execution processes.[33]

2. CFTC and Bitcoin

The CFTC has not announced plans to levy mandates that are particular to smart contracts. Various products are eligible for CFTC oversight, which may include commodities, forward contracts, futures contracts, options on futures contracts, and swipes. Included in this list of commodities is bitcoin, as the CFTC determined that

---

31 Lab CFTC, *A CFTC Primer on Virtual Currencies*, http://www.cftc.gov/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf (last visited Jan 2, 2018).

32 Commodities Future Trading Commission. A primer on smart contracts. *Commodities Future Trading Commission*, 2018.

33 Jeremy Wall, *CFTC Releases Smart Contract and Blockchain Technology Primer* (2018), https://www.investinblockchain.com/cftc-blockchain-technology-primer/. (last visited Jul 31, 2019).

bitcoin is a commodity.[34] It did so following an order against Coinflip, a now-defunct institution that was based in San Francisco, California, that offered bitcoin trading on its platform, called Derivabit. The platform connected buyers and sellers of bitcoin options contracts. The CFTC asserted jurisdiction over Derivabit's activities by determining that "bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities." [35] Based upon this finding, the CFTC found that Derivabit had illegally offered commodity options without being registered as an exchange or swap execution facility with the Commission.[36]

By identifying bitcoin as a commodity, the CFTC will be better able to oversee falsified efforts in virtual communications where both bitcoins and bitcoin derivatives are exchanged. Bitcoin derivates offer the chief medium by which an entity can steady the agreed-upon value of their bitcoins, even when the markets are turbulent.

3. Other CFTC Actions and Commissioner Speeches

In addition to the actions on smart contracts and bitcoin, the CFTC also engages in innovation, bringing together innovators, market participants, and thought leaders from industry, academia and regulatory authorities, as well as the general public to examine the wide range of fintech developments impacting markets, such as hosting FinTech Forward 2018: Innovation, Regulation and Education, a conference that featured discussions on cryto assets, machine learning, cloud technologies, regtech, and other emerging financial technologies.[37]

As the chairman of the CFTC, Christopher Giancarlo noted during a Senate budget hearing that the CFTC must adapt to an environment that may be more difficult to regulate given the "extraordinary pace of exponential technological change, the disintermediation of traditional actors and business models, and the need for technological literacy and big data capability."[38] Giancarlo suggested that one way to do this was to be a quantitative regulator, running independent data analysis "across different data sources, including decentralized blockchains and networks."[39]

---

34 Jared Paul Marx, *Bitcoin as a Commodity: What the CFTC's Ruling Means* (2015), https://www.coindesk.com/bitcoin-as-a-commodity-what-the-cftcs-ruling-means.

35 *ORDER INSTITUTING PROCEEDINGS PURSUANT TO SECTIONS 6(c) AND 6(d) OF THE COMMODITY EXCHANGE ACT, MAKING FINDINGS AND IMPOSING REMEDIAL SANCTIONS, Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan;* CFTC Docket No. 15-29, https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalplea ding/enfcoinfliprorder09172015.pdf (last visited Jul 31, 2019).

36 *Id.* at 4. Most recently, Judge Weinstein of the U.S. District Court for the Eastern District of New York affirmed the Commission's conclusion that virtual currencies were commodities subject to the Commission's jurisdiction in a Preliminary Injunction Order.

37 Basic Challenge | U.S. COMMODITY FUTURES TRADING COMMISSION, (2018), https://www.cftc.gov/PressRoom/PressReleases/7810-18. Subject: Finance and accounting (last visited Jul 31, 2019).

38 Testimony of Chairman J. Christopher Giancarlo before the House Committee on Agriculture Subcommittee on Commodity, Energy and Credit, Washington D.C., May 2019.

39 *Id.*

Giancarlo also noted at the 4th Annual DC Blockchain Summit that "the potential of the blockchain and its impact on financial markets has been a key focus of ours."[40] With thoughts on the relationship between technology, regulation, and markets, he took stock of the current state of blockchain and renewed a focus on how it can impact and improve markets. Admitting that DLT is likely to have a broad and lasting impact in payments, banking, securities settlement, title recording, cyber security, and trade reporting and analysis,[41] Giancarlo leads the CFTC and takes affirmative steps to craft a modern regulatory approach, which is predicated on four key elements: (1) adopting an exponential growth mindset, (2) creating an internal Fintech stakeholder, (3) becoming a quantitative regulator, and (4) embracing market-based solutions.[42] This approach is consistent with the "no-harm approach" to DLT he proposed three years ago.[43]

Before the DC Blockchain Summit, Commissioner Brian Quintenz expressed his concerns regarding cryptocurrency futures, which include the futures contract's financial integrity and price volatility.[44] He also noted that the initial margin for bitcoin futures contracts has performed as required and that it is important to continuously monitor and regularly re-evaluate its performance. Looking forward, Quintenz urged that an independent body for cryptocurrencies must step up, establish, and enforce the rule of play and believes that a private, cryptocurrency oversight body could achieve goals of global significance.

C. The Department of Treasury's Financial Crimes Enforcement Network

The FinCEN was established in April 1990 by Treasury Order Number 105-08. Its earliest objective was to deliver a comprehensive analytical and intelligence network using multiple sources to aid the government in identifying, investigating, and prosecuting money laundering, in addition to other financial crimes, both domestically and internationally.

---

[40] J. Christopher Giancarlo, *Special Address of CFTC Commissioner J. Christopher Giancarlo Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium-"Regulators and the Blockchain: First, Do No Harm"* (2016), https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-13. Subject: Law

[41] Written Testimony of Chairman J. Christopher Giancarlo before the Senate Banking Committee | U.S. COMMODITY FUTURES TRADING COMMISSION, , https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo37 (last visited Jul 31, 2019). [42] Remarks of Chairman J. Christopher Giancarlo at the 4th Annual DC Blockchain Summit | U.S. COMMODITY FUTURES TRADING COMMISSION, *supra* note 35.

[43] Special Address of CFTC Commissioner J. Christopher Giancarlo Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium |Basic Challenge | U.S. COMMODITY FUTURES TRADING COMMISSION, (2016), https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-13 . (last visited Jul 31, 2019). [44] Keynote Address of Commissioner Brian Quintenz before the DC Blockchain Summit | U.S. COMMODITY FUTURES TRADING COMMISSION, , https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz8#P18_4322 (last visited Jul 31, 2019).

In October 2001, the USA Patriot Act made FinCEN a Treasury bureau, and its mission is still to detect and stop money laundering in two major ways. First, FinCEN collaborates with members of the financial community to identify and discourage money laundering. This includes specific counter-money laundering laws like the Bank Secrecy Act (BSA), which mandates reporting and recordkeeping by financial institutions, including banks, and helps sustain a money trail for investigators to follow. In addition, the act mandates the disclosure of suspicious currency transactions, which could then prompt criminal inquiries. The second way FinCEN combats money laundering is by delivering intelligence and sharing information to and between law enforcement.

In 2011, FinCEN issued its 2011 MSB Final Rule, which identifies a currency amenities institution as an individual who does business at least partly in the United States, candidly, or through a negotiator, representor, or organization that operates as a financial transmitter. A financial transmitter, in this context, is as an individual who grants financial exchange services, or another entity involved in the handover of assets.

Recently, FinCEN released its regulations to certain business models involving convertible virtual currencies (CVCs).[45] This guidance was provided to address inquiries offered by economic institutes, government, and oversights about the supervision of several types of institutions associated with CVCs. In addition to this, FinCEN also released its advisory on illicit activity involving convertible virtual currency to help institutions recognize and record information about untrustworthy activities associated with illegal manipulation of CVCs for money washing, permissions circumvention, and other illegal funding resolves.[46]

Kenneth A. Blanco, the FinCEN director, in a speech at Morehouse College in February of 2019, argued that FinCEN had to be cognizant of the new technologies that impact payment systems, in large part because such transformations also produce new type of financial crime and financial criminals. "As a regulator in this space, and a protector of our national security, FinCEN is in front of the curve and vigilant to ensure that innovative products and services such as virtual currency payment systems are not exploited to support and facilitate terrorism, or used by criminals to harm others," he argued.[47]

Blanco also noted that FinCEN was one of the first agencies to release regulations and give guidance in regard to virtual currency, and that its regulatory reach is both domestic and international, regardless of the physical location of money transmission. Moreover, FinCEN launched a collaboration with the IRS to more closely examine virtual currency money services businesses, including trading

---

45 FIN-2019-G001- *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (last visited Jul 31, 2019).

46 FIN-2019-A003 - *Advisory on Illicit Activity Involving Convertible Virtual Currency*, (2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-09/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf. (last visited Jul 31, 2019).

47 Remarks of Kenneth A. Blanco to Morehouse College, Atlanta, GA., February 2019.

platforms, virtual currency kiosks, peer-to-peer exchangers, and administrators.

D. The Consumer Financial Protection Bureau

The CFPB was created by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, and its main mission is to regulate financial services and products for consumers. It is tasked with defending and informing consumers about financial services and products. To do so, this regulatory agency assists consumer finance markets function more capably, as well as postulates—and enforces— specific rules, thereby encouraging consumers to have confidence and control of their financial lives.

In 2019, acting head Mick Mulvaney created the Office of Innovation to focus on consumer-friendly innovation, exploring blockchain and cryptocurrencies. To achieve the statutory mandate to promote competition, innovation, and consumer access with financial services, the new office will create policies to facilitate innovation, engage with entrepreneurs and regulators, and review outdated or unnecessary regulations.[48] Mulvaney also announced that the CFPB would introduce a regulatory sandbox to support blockchain and other financial technology innovation.[49] As Mulvaney told The Wall Street Journal, the CFPB will play a role in helping companies advancing these technologies and the byproduct of those technologies, specifically focusing on blockchain-based platforms, cryptocurrencies, individual micro-lending, and other private currencies.[50]

E. Federal Trade Commission

The mission of the FTC is "protecting consumers and competition by preventing anticompetitive, deceptive, and unfair business practice through law enforcement, advocacy, and education without unduly burdening legitimate business activity." [51] FTC's work is performed by the Bureaus of Consumer Protection, Competition and Economics. That work is aided by the Office of General Counsel and seven regional offices.

On March 16, 2018, the FTC announced a lawsuit against four individuals, alleging that they promoted one or more fraudulent "chain referral schemes."[52] In this

---

48 Felix Shipkevich, *CFPB Launches Office of Innovation, Explores Blockchain, Cryptocurrency*, MONEY TRANSMITTER LAW (2018), https://moneytransmitterlaw.com/cfpb-office-of-innovation- cryptocurrency/ (last visited Jul 31, 2019).

49 CFPB Office of Innovation proposes "disclosure sandbox" for companies to test new ways to inform consumers, , CONSUMER FINANCIAL PROTECTION BUREAU , https://www.consumerfinance.gov/about-us/blog/cfpb-office-innovation-proposes-disclosure- sandbox-companies-test-new-ways-inform-consumers/ (last visited Jul 31, 2019).

50 Shipkevich, *supra* note 43.

51 About the FTC, FEDERAL TRADE COMMISSION (2013), https://www.ftc.gov/about-ftc (last visited Aug 18, 2019).

52 FTC Shuts Down Promoters of Deceptive Cryptocurrency Schemes, FEDERAL TRADE COMMISSION

case, the FTC filed against Bitcoin Funding Team and My7Netwek, which used various social media and conference calls to promote chain referral schemes with the promise of a payment of Bitcoin or Litecoin. These schemes falsely promised that participants could earn large returns by paying cryptocurrency such as bitcoin or Litecoin to enroll in the schemes. In fact, only a few would benefit while the majority of participants would fail to recoup their initial investments. This was the FTC's first chain referral case involving cryptocurrency. "This case shows that scammers always find new ways to market old schemes, which is why the FTC will remain vigilant regardless of the platform or currency used," said Tom Pahl, acting director of the FTC's Bureau of Consumer Protection.[53] The FTC brought its first cryptocurrency- related case in June 2015, another in February 2016, and held a public forum on blockchain technology in March 2017.[54]

On the same day, the FTC also published a press release announcing the formation of Blockchain Working Group and outlining its structure.[55] The CFTC expects that fraudsters could dress up old schemes with cryptocurrencies, affecting the FTC's consumer protection and competition mission in five other ways: bad actors' seeking payment in cryptocurrency, the emergence of new schemes, defendant's assets obtained through misconduct, incumbent companies' seeking to hobble potential competitors through regulatory burden, and blockchain's capability of providing new solutions to micropayments, data privacy, and secure identity.[56] The working group has at least three goals. The first is to build on FTC staff expertise in cryptocurrency and blockchain technology through resource sharing and by hosting outside experts. Second, it hopes to facilitate internal communication and external coordination on enforcement actions and other related projects. And third, it aims to serve as an internal forum for brainstorming potential impacts on the FTC's dual missions and how to address those impacts.[57]

F. The Internal Revenue Service

The primary goal of the IRS is as a tax administrator, collecting individual income taxes and employment taxes. In addition, the agency promotes its role as an educator of the taxpayers, helping them understand and fulfill their tax responsibilities, as well as enforcing the law equally and justly.

With respect to blockchain technology, not only did the IRS present on Bitcoin, cryptocurrency, and blockchain technology more generally in its 2018 Tax

---

(2018), https://www.ftc.gov/news-events/press-releases/2018/03/ftc-shuts-down-promoters-deceptive-cryptocurrency-schemes (last visited Aug 18, 2019).

53 *Id.*

54 Neil Chilson, *It's time for a FTC Blockchain Working Group | Federal Trade Commission* (2018), https://www.ftc.gov/news-events/blogs/techftc/2018/03/its-time-ftc-blockchain-working-group . Subject: Finance and accounting (last visited Aug 18, 2019).

55 *Id.*

56 *Id.*

57 *Id.*

Forum, but it has also issued guidance from Keith A. Aqui of the Office of Associate Chief Counsel, on the tax treatment of transactions using virtual currencies, such as Bitcoins or other similar currencies.

In general, the guidance notes that the sale or other exchange of virtual currencies, or the use of virtual currencies to pay for goods or services, or holding virtual currencies as an investment, generally has tax consequences that could result in tax liability, and applies to individuals and businesses that use virtual currencies. More specific guidelines are listed below.

For federal tax purposes, virtual currency is considered property. In this way, all conventional tax principles that apply to property transactions also apply to transactions using virtual currency. However, virtual currency is not treated as currency that could generate foreign currency gain or loss for U.S. federal tax purposes. In addition, the IRS advises that a taxpayer who receives virtual currency as payment for goods or services must, in computing gross income, include the fair market value of the virtual currency, measured in U.S. dollars, as of the date that the virtual currency was received. The basis of virtual currency that a taxpayer receives as payment for goods or services in is the fair market value of the virtual currency in
U.S. dollars as of the date of receipt.

Therefore, taxpayers will be required to determine the fair market value of virtual currency in U.S. dollars as of the date of payment or receipt. If a virtual currency is listed on an exchange and the exchange rate is established by market supply and demand, the fair market value of the virtual currency is determined by converting the virtual currency into U.S. dollars (or into another real currency, which in turn can be converted into U.S. dollars) at the exchange rate, in a reasonable manner that is consistently applied.

Finally, taxpayers may be subject to penalties for failure to comply with tax laws. For example, underpayments attributable to virtual currency transactions may be subject to penalties, such as accuracy-related penalties under section 6662. In addition, failure to timely or correctly report virtual currency transactions when required to do so may be subject to information reporting penalties under section 6721 and 6722. However, penalty relief may be available to taxpayers and persons required to file an information return who are able to establish that the underpayment or failure to properly file information returns is due to reasonable cause.

G. Federal Bureau of Investigation and the Department of Justice's Criminal Division

The DOJ is a federal executive department of the U.S. government, responsible for the enforcement of law and administration of justice. Mythili Raman, acting assistant attorney general at Criminal Division of the DOJ, in her 2-13 testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, stated that "The department [DOJ] has two primary law enforcement interests in virtual currency: 1) deterring and prosecuting criminals using virtual currency systems to move or hide money that is used to facilitate, or is

derived from, criminal or terrorist acts, i.e., money laundering; and 2) investigating and prosecuting those virtual currency services that themselves violate laws aimed at illegal money transmission and money laundering."[58]

The DOJ administers several federal law enforcement agencies, including the FBI. In the blockchain space, the role of the FBI is to investigate a variety of federal crime that may involve the use of blockchain, especially those in the cryptocurrency space, and to support the prosecution of those who commit related crimes.

The FBI has worked toward prosecuting entities involved in criminal practices related to virtual currencies. For instance, many law enforcement agencies have started prosecuting entities that are thought to have used virtual currencies to encourage money laundering or related criminal practices.[59] A major case involving virtual currencies occurred when the FBI worked to close the Silk Road in October 2013. This was a virtual market where users bought, sold, and exchanged illegal items, like weapons and narcotics, and things like hit man services, through the dark Web. [60] The FBI has also increased its presence by partaking in dialogue and workgroups focused on money laundering with virtual currency and related issues.[61]

II. EX-POST REGULATORY IMPACT ASSESSMENT

The second part of the article aims to evaluate whether the actions (i.e., issuing interpreting rules, issuing guidance, piloting initiatives, or taking enforcement actions) have generated their intended effects. Following the steps of the modified RIA, this sections below first identify the problems before any action was taken, then analyze the objectives of existing regulatory regimes toward blockchain and its applications, and further assess whether the objectives have been fulfilled.

A. What Were the Problems Before Any Regulatory Action was taken?

This section includes a discussion of the major problems that prompted regulatory actions. Although regulatory agencies have been releasing guidance, such as investor alerts and bulletins, and their officials have been expressing regulatory opinions and concerns at various occasions since the appearance of bitcoin (2009), the real regulatory actions that have great impacts on the investment markets did not start until two cases in recent years. One is the CFTC's settlement with the Coinflip, which marketed bitcoin derivatives, in September 2015. The other case is the SEC's

---

58 STATEMENT OF MYTHILI RAMAN BEFORE THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE FOR A HEARING ENTITLED "BEYOND THE SILK ROAD: POTENTIAL RISKS, THREATS AND PROMISES OF VIRTUAL CURRENCIES," , https://www.hsgac.senate.gov/imo/media/doc/Opening%20Statement- Carper-2013-11-18.pdf (last visited Aug 13, 2019).

59 UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, *Virtual Currencies, Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*, https://www.gao.gov/assets/670/663678.pdf (last visited Aug 7, 2019).

60 *Id.*

61 *Id.*

report on The DAO in July 2017. In addition to the investment markets, FBI's taking down of Silk Road in 2013 and Silk Road 2.0 in 2014 represent a shift in the law enforcement agency's attention to the illegal use of cryptocurrencies. These law enforcement actions have affected the economy and market participants in general.

The reason I see these cases as the starting points of regulatory agencies' cautious and active engagement with the blockchain space is that they have brought the true impacts to market participants. Before 2017, cryptocurrency-related activities were the major form of blockchain's engagements with the market, involving a great number of participants, which could post dramatic threat to financial integrity. Relative clear rules as to whether trading bitcoin derivatives was legal and trading other cryptocurrencies would be treated as securities transactions gave market participants a general idea as to which action could lead to punishable results. Although rules become clearer as more cases appeared and have been handled, these two cases are the milestones that affect the blockchain space enormously.

Thus, a rough period from 2013 to 2017 is the time that I see regulatory agencies starting to substantively perform oversight and enforcement in the blockchain space. The problems I identify in this session happened in or before this period. Major problems centered around a lack of knowledge and skills in the blockchain and crypto fields, and criminals preying on the hype of cryptocurrencies for illegal activities, which resulted in fraud and scams in the cryptocurrency markets, law enforcement difficulties, and immature blockchain products and services.

1. Fraud and Scams in the Cryptocurrency Market

Many different types of fraud and scams occur in the cryptocurrency marketplace. Some are securities-related frauds. Some are illegal transactions, such as using cryptocurrencies to purchase narcotics or firearms, and using cryptocurrencies for money laundering, illegal gambling (online and offline wager settlements), and tax evasion. One of these securities frauds includes the advance fee fraud, in which scammers ask investors to provide a phony fee in exchange for profit, currency, stock, or warrantees. Simply put, it is an agreement for investment that promises a high return in exchange for funds. Similar to the Howey Test, scammers promise entities with high virtual currency with a return on investment as high as 20% to 50% from minimal-to-no risk involved. As in the case with the Howey trial, this is oftentimes conducted with people who are neither investors nor experts in bitcoin or virtual currency themselves and do not have a developed understanding about the real level of risk involved. Oftentimes, these scammers are operating from foreign localities, and can easily transfer the virtual funds received to other entities with a trail that is difficult to trace.

Market manipulation is another one of the main ways that fraudsters seek to profit in the cryptocurrency market. When companies partake in market manipulation, they swindle investors by directing or unnaturally disturbing the marketplace for a security. Manipulation can happen much more easily in the case of cryptocurrencies and take place in a variety of forms. Unlike the securities market,

where strict regulations exist as to which information a company could publish before an IPO, the absence of any regulation in the cryptocurrency market enables scammers to constantly to publish deceitful but appealing information about certain cryptocurrencies on social media intended to impact the quantity of or need for these cryptocurrencies, such as unethically hindering the amount of a cryptocurrency to the public, or setting cost or dealings to develop an incorrect idea of the need for this cryptocurrency, thus inducing investors to purchase these cryptocurrencies.

A pump-and-dump scheme is part of a more complex plan of market manipulation on the targeted security. This type of scheme crafts a false pressure to purchase a specified security and tends to involve low-volume exchanges in the over-the-counter securities market that are chiefly regulated by the perpetrators. The over-the-counter securities market refers to securities that are sold, bought, and traded that are not listed on a verified exchange, such as the New York Stock Exchange, indicating the exchange has less guidance. By consequently creating the false notion of growing trade, thus increasing demand, the perpetrator also increases the price of the security, or the "pump," which is quickly sold into the overstated marketplace by the criminals, or the "dump."[62] This can happen more easily with cryptocurrencies, since scammers have unlimited access to virtual spaces, such as social media, and can constantly solicit investors to buy their cryptocurrencies through false news reports or posts that create false urgency that tell subscriber to buy.[63] Once the price of the cryptocurrencies reaches a certain level, the perpetrators would sell all of their cryptocurrencies into public market, the prices would fall, and investors would essentially possess valueless cryptocurrencies.

In addition, cryptocurrency theft and using cryptocurrencies for illegal transactions, such as purchasing narcotics or firearms and money laundering, are also prevalent in the crypto field. According to a Reuters report on bitcoin fraud, there were 26 bitcoin-related thefts conducted between June 2011 and April 2017, amounting to $3.5 billion in value. The major reason to use cryptocurrencies for money laundering is that it is possible to have users remain completely anonymous on the network, allowing users to transfer and withdraw money without detection. Using cryptocurrencies meets the purpose of making the origin of large amounts of money generated by criminal activities untraceable. Money from drug trafficking or terrorist funding could appear to have come from a legitimate source.

Elaborating on a discussion mentioned previously, the Silk Road, an online black market and the first modern darknet market, best known for the selling and exchanging of illegal drugs, was shut down by the FBI in October 2013. [64] Shortly

---

62 Market Manipulation ("Pump and Dump") Fraud, FEDERAL BUREAU OF INVESTIGATION , https://www.fbi.gov/scams-and-safety/common-fraud-schemes/market-manipulation-pump-and- dump-fraud (last visited Aug 2, 2019).

63 Basic Challenge | *U.S. COMMODITY FUTURES TRADING COMMISSION*, (2018), https://www.cftc.gov/PressRoom/PressReleases/pr7697-18. Subject: Finance and accounting 2019. 64 Case 76: Silk Road (Part 1), CASEFILE: TRUE CRIME PODCAST (2018), https://casefilepodcast.com/case-76-silk-road-part-1/ (last visited Aug 7, 2019).

after, the Silk Road II was launched, which was run by a former administrator of Silk Road. Shortly after, in November 2014, the FBI seized dozens of users of the "dark net," including Silk Road II, operating on the anonymous Tor network. Tor network is free and open-source software for enabling anonymous communication. Using Tor makes it more difficult to trace Internet activity to specific users. This activity includes website visits, online posts, messaging, and other forms of communication.[65] In these darknets, participants used bitcoin to conduct illegal transactions. On June 23, 2013, it was first reported that the Drug Enforcement Administration seized 11.02 bitcoin, then worth a $814 million.[66] The FBI initially seized 26,000 bitcoins from accounts on Silk Road, worth approximately $3.6 million at the time. In total, the FBI has seized close to $34.5 million from the Silk Road as of October 2013.[67] In October 2013, the FBI reported that it had seized 144,000 bitcoins, worth $28.5 million, and that the bitcoins belonged to Ulbricht, the founder of Silk Road. [68] Another 144,342 bitcoins were found on Ulbricht's computer, amounting roughly $87 million.[69] These were just some illegal transactions being reported, while many were still veiled.

Cryptocurrencies could simplify money laundering while complicating enforcement.[70] Under one general model, money laundering has three basic stages steps: 1) placement, 2) layering, and 3) integration, as showed in the chart below. [71] Placement or promotion includes most effort to initially make the funds less

---

As casefile explained, the Silk Road was an ancient network of trade routes that started in China in the 2nd century B.C. Via a combination of roads and sea routes, goods like silk, paper, and spices were transported from the producers in Asia to markets in Europe. Eventually, it wasn't just goods that were traded—there were also ideas, customs, religions, and even diseases. The Silk Road expanded throughout different continents and civilizations for several centuries. It connected Asia, Europe, Africa, and the Middle East, as a marketplace across the world. But the Silk Road in this context refers to a black market known for selling illegal drugs.

65 Jonathan D. Glater, *Privacy for People Who Don't Show Their Navels*, THE NEW YORK TIMES, January 25, 2006, https://www.nytimes.com/2006/01/25/technology/techspecial2/privacy-for-people-who-dont-show-their-navels.html (last visited Aug 7, 2019).

66 Adrianne Jeffries, *Drug Enforcement Administration seizes 11 Bitcoins from alleged Silk Road dealer*, THE VERGE (2013), https://www.theverge.com/2013/6/26/4468302/drug-enforcement-agency- seizes-11-bitcoins-in-south-carolina-bust-silk-road (last visited Aug 7, 2019).

67 Andy Greenberg, *FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road,* , https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#4c148b4f2765 (last visited Aug 7, 2019).

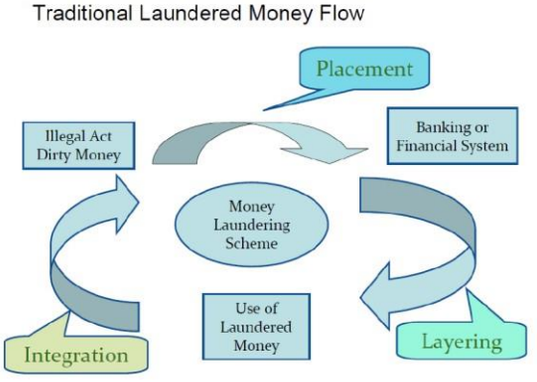
68 *Id.*

69 Peter Svensson, *US Marshals to auction seized bitcoin* - Washington Times, , https://www.washingtontimes.com/news/2014/jun/12/us-marshals-to-auction-seized-bitcoin/ (last visited Aug 7, 2019).

70 JOHN W. BAGBY, DAVID REITTER & PHILIP CHWISTEK, *An Emerging Political Economy of the BlockChain: Enhancing Regulatory Opportunities* (2018), https://papers.ssrn.com/abstract=3299598 (last visited Aug 10, 2019). at 57

71 Report To Congress, In Accordance with §356(C) Of The USA Patriot Act, Secretary of the Treasury, Board of Governors of the Federal Reserve System, Securities and Exchange Commission, Dec. 31, 2002 at 7, accessible at http://www.fincen.gov/news_room/rp/files/356report.pdf

suspicious by having them enter the financial system after initial unlawful acquisition. The next step is laying, which separates the illegal proceeds from their source through multiple and complex financial transactions, including wire transfers, monetary instruments, and asset purchases or sales. The third step is integration, which reintroduces the funds into the economy for ultimate use; this is essentially a reentry into the legitimate economy. [72] Cryptocurrencies can simplify money laundering by abbreviating the complex layering process, because the anonymity of cryptocurrency transactions makes the appearance of further legitimizing unnecessary.



Source: Report to Congress[73]

2. Law Enforcement Difficulties

Blockchain technology has posed various challenges for law enforcement agencies, especially when blockchain encounters the financial sector. The anonymous and decentralized characteristics of blockchain cause difficulties in de-identification and transability. Blockchain's cross-jurisdictional nature also creates inconvenience for law enforcement to investigate and prosecute cross-border crimes. Because of the encrypted, decentralized, and transnational character of blockchain technology, said technology can be used in illegal ways and for illegal purposes. However, given the anonymity that the blockchain provides, it may be much more difficult for law enforcement and their agencies to ascertain, and later prosecute, those who engage in illegal acts. In part, this is because blockchain technology is not only anonymous, but also decentralized, which makes it more challenging for law enforcement or the government to intercept communications through channels. Given the ease with which blockchain allows for encryption and the use of end-to-end encryption (which allows for data to be encrypted as it travels between two points), messages can only be unlocked using a secret key that is given

---

72 BAGBY, REITTER, AND CHWISTEK, *supra* note 67. at 58
73 *Id.*

to two parties. This type of security, therefore, could obfuscate the use of legal and legitimate surveillance that is needed and used for both law enforcement and prosecution. [74]

Such difficulties were similarly faced by the telecommunications industry two decades previously when digital telephone exchanges became popular, resulting in challenges for law enforcement in pursuit of wiretaps. The government quickly passed the Communications Assistance for Law Enforcement Act, mandating these companies adjust and design their services, facilities, and equipment to guarantee that those technologies allow for built-in surveillance capabilities, allowing federal agencies to wiretap any internet, telephone, and VoIP traffic. However, such a fix is more difficult with blockchain technology since, unlike telecommunication networks, there is no middleman for the government to regulate. Thus, communication networks are more challenging to break, while it is simultaneously easier to coordinate cybercrimes and even cyberwarfare by bad actors.[75]

The Government Accountability Office also found that law enforcement agencies studying and indicting wrongdoings that include virtual currencies may have to depend on assistance from global cohorts who may work under dissimilar governing and lawful administrations because of the unique property of the virtual currency systems, which allow cross-border payments or transactions.[76] Major parts of cryptocurrency activities happen online and can be assessed globally. Many of the cryptocurrency transactions could occur in different jurisdictions, such as using one platform to exchange traditional currencies to cryptocurrencies, conducting cryto-to-cryto exchanges with another platform, and storing crypto assets in a wallet with a third-party service provider. Many of these service providers are located outside of the U.S., so domestic BSA and anti-money-laundering requirements are not applicable. As to those partial activities that happen in the U.S., regulators or law enforcement agencies may need international cooperation to investigate and prosecute crimes, such as assessing criminals, seizing properties, and making arrests. However, international cooperation may not always be viable due to the high cost, different legal regimes, and the political climates between two countries.

3. Immature Blockchain Products and Services

Blockchain companies have progressed since the blockchain first presented in the marketplace in 2009. Daley at Built In has rounded up 31 U.S.-based companies using blockchain that he thinks can be used to prove that blockchain is an

---

74 Aaron Wright and Primavera De Filippi. "Decentralized blockchain technology and the rise of lex cryptographia." *Available at SSRN 2580664* (2015).

75 *Id.*

76 UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, *Virtual Currencies, Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*, https://www.gao.gov/assets/670/663678.pdf (last visited Aug 7, 2019).

avenue for improving the future. [77] Some of the companies are described as predominantly blockchain companies, while others are existing companies that have adopted the new technology to expand their range of services.

As indicated on the list of these 31 companies, the scope of exploring blockchain products and services is limited. In 2012, many companies' efforts revolved around buying and selling cryptocurrencies and connecting buyers. In 2014, the companies and services became a bit more complex, with blockchain-related products offered to improve the access or experience of other phenomenon or services. For instance, in 2014, Voatz was founded as a mobile voting platform used during elections, and a year later, Lemonade was founded to help users receive renters and homeowner's insurance information. This shift indicated that the uses of blockchain was changing. Ironically, the uses of blockchain that followed 2015 appeared to transition back to the original uses of the technology, which was to connect buyers and sellers of cryptocurrencies, in addition to allowing users access to loans and means of investing in emerging markets. This teetering between original uses and growing complexity may signify that knowledge of blockchain and its uses in the consumer markets remain unexplored.

There is more than one way to gain exposure to blockchain innovation. Forbes has looked into the 2018's Forbes Global 2000 list of the largest public companies, revealing that "not only are all ten of the largest public companies in the world exploring blockchain, but at least 50 of the biggest names on the list have all made their own mark on technology first inspired by bitcoin." [78] Among these 50 companies, 21 are U.S. companies. Most of them are tech companies or banks.

Looking into their experiments with blockchain, many of these U.S. companies were still at the planning or exploration stage as of 2018. For example, Oracle had been preparing to launch its own enterprise blockchain platform. MetLife, the insurance giant, has partnered with IBM and insurance tech company Majesco, to build a blockchain platform for insurance. Ford Motor Company, the auto giant, co- launched a blockchain research group for the auto industry. Goldman Sach Group had planned to open its own bitcoin trading desk. Bank of America was working to automate the process of creating letters of credit using the Ethereum blockchain. Berkshire Hathway, Berkshire subsidiary BNSF Railroad, and fine jewelry subsidiary Richline Group, were exploring blockchain to streamline their supply chains. Pfizer, a pharmaceutical giant, was in the early stages of a project with Chronicled, a blockchain startup, for supply chains.

Some of them were building infrastructure basis or backed other companies and had not have mature applications or implementations. For example, Prudential Financial, largely working behind the scenes, was a backer of influential Digital Currency Group. Amazon offered cloud integrations for a number of blockchains and

---

77 Sam Daley, *31 blockchain companies paving the way for the future*, BUILT IN , https://builtin.com/blockchain/blockchain-companies-roundup (last visited Aug 24, 2019).

78 Michael Del Castillo, *Big Blockchain: The 50 Largest Public Companies Exploring Blockchain*, Forbes, https://www.forbes.com/sites/michaeldelcastillo/2018/07/03/big-blockchain-the-50-largest- public-companies-exploring-blockchain/#22c81a1d2b5b (last visited Aug 25, 2019).

recently partnered with Ethereum startup ConsenSys. In spite of clearing bitcoin futures contracts for its customers, Morgan Stanley issued a report the negative impacts of bitcoin mining on the environment. Comcast, the telecommunications giant backed Boldstart Ventures, invests in enterprise blockchain startups.

Only a few companies had seen a slightly greater progress with blockchain innovation. IBM had open-sourced the widely used Hyperledger Fabric and is a driving force behind multiple blockchain initiatives. Walmart, since an early prototype to use Hyperledger Fabric on the pork supply chain, the global grocer, had expanded its blockchain work to other supply chains. Microsoft, the software giant, was among the first to monetize blockchain services, and now works with a number of blockchains via its Azure platform. Apple had filed a patent for using blockchain technology to timestamp data. JP Morgan Chase had contributed blockchain platform Quorum to the open-source community.

From these companies' experiments with blockchain innovation, we can see many of them had been beyond connecting buyers or sellers of cryptocurrencies or building cryptocurrency trading platforms. The scope of work became more diverse, extending to supply chains, insurance, membership rewards, tracking securitized mortgages, and automating the process of creating letters of credit. However, implementations had been sluggish because many of these were at the early stage experimentations—some solutions were still in the nascent proof-of-concept stages. Some institutions just started building research groups or purely backing up other companies or blockchain projects. Worse, some experiments have been controversial. For example, IBM's Hyper Ledger Fabric is challenged because it does not require a true consensus mechanism at all.[79] "In effect, IBM's "blockchain" is nothing more than a glorified time-stamped list of entries.[80] Thus, the market barely could see mature blockchain products or services, and widespread adoptions are still far away.

B. What Are the Objectives of the Existing Blockchain Regulatory Regime?

The regulatory actions taken by regulatory agencies toward blockchain technology and its applications, at a higher level, share the same goals of financial regulation, such as protection of public claims, the elimination of externalities from the failures of intermediaries, adjunct to law enforcement, and the justification of political economy.[81] The goals of each regulatory agency have been decided when they were created to deal with certain issues. Thus, each regulatory agency may lay

---

79 Stuart Popejoy, *IBM's Hyperledger isn't a real blockchain — here's why*, PODIUM | THE NEXT WEB (2019), https://thenextweb.com/podium/2019/05/05/ibms-hyperledger-isnt-a-real-blockchain-heres-why/ (last visited Aug 25, 2019).

80 *Id.*

81 Financial Regulation: Law and Policy (University Casebook Series): Michael S. Barr, Howell E. Jackson, Margaret E. Tahyar: 9781634592956: Amazon.com: Gateway, , https://www.amazon.com/Financial-Regulation-Policy-University-Casebook/dp/1634592956/ref=sr_1_2?crid=3KGJ44P6EKU20&keywords=financial+regulation+law+and+policy&qid=1565965783&s=gateway&sprefix=financial+regulation+%2Caps%2C140&sr=8-2 (last visited Aug 16, 2019). At 72

emphasis on achieving specific goals under these broad objectives of financial regulation. At a specific level, the existing blockchain regulatory regime should address issues unique to blockchain in the financial markets.

To identify the objectives of the existing blockchain regulatory regime, two major considerations are the mission of a regulatory agency and how to address blockchain-related problems following its mission. No matter how detailed and concrete regulations, rules, or guidelines are, each of regulatory agencies constantly follows its mission entrusted by law. This refers to the function of this regulatory agency in the financial markets. Actions taken to deal with problems in the blockchain space is a specific case of implementing this mission.

For instance, the mission of the SEC is to protect investors, to maintain fair, orderly, and efficient markets, and to facilitate capital formation. When dealing with problems of blockchain interrupting its regulatory realm, the SEC would first examine how blockchain and its related activities, such as using blockchain to record ownership of shares, using cryptocurrencies to raise funds, and making crypto investments, expose investors to risk, mess up fair, orderly and efficient markets order, and hinder capital formation. The SEC then would intervene in the markets disturbed by blockchain. One method of intervention is to issue policies and regulations to require further disclosure on blockchain and its relevant products, organizations, or activities.

After going through major regulatory actions in the blockchain space issued by regulatory agencies and understanding their particular mission in the markets, the article explains four major objectives: 1) maintaining a fair and efficient market, 2) protecting investors and consumers,3) assisting criminal enforcement, and 4) fostering technology innovation.

1. Maintaining a Fair and Efficient Market

Financial markets consist of various components, such as securities markets, derivatives markets, banking, and insurance markets. Different components of financial systems have at times been at odds with one another and at other times have combined forces or created new organizational forms or financial products. [82] The markets blockchain gets involved are securities markets and derivatives markets, thus far. Blockchain seems to bring together regulators of securities and derivatives markets instead of stirring war between them.

Regulators in these markets share the same goal: to ensure a fair and efficient market. As the major regulatory agency of the securities market, the SEC, as indicated, was created with a three-part mission: 1) to protect investors; 2) maintain fair, orderly, and efficient markets; and 3) facilitate capital formation.[83] As the major regulatory agency of the derivates markets, the mission of CFTC is to foster open, transparent, competitive, and financially sound markets with an aim to protect market

---

82 *Id.*at 32

83 *The Role of the SEC* | Investor.gov, https://www.investor.gov/introduction-investing/investing- basics/role-sec, (last visited Aug 14, 2019).

users and their funds, consumers, and the public from fraud, manipulation and abusive practices related to derivatives and other products that are subject to the Commodity Exchange Act.[84]

To maintain a fair and efficient market, the first enquiry is what encumbers a fair and efficient market. A theory behind this is the Efficient-Market Hypothesis (EMH), enunciated by professor Eugene Fama in 1969. [85] According to this theoretical approach, a market is efficient if all the players acting within it have the same information. If that happens, no player would be able to gain advantage from the information obtained, or to predict future developments of prices of an asset from the information available.[86] Thus, no fair access to information is a major reason why the market is inefficient. Although this is not a perfect approach, as it was criticized by the behavioral finance school that sees finance from a broader social science view, including psychology and sociology.[87] The EMH still has evidenced a great deal of consistency in the way it understand the ability of financial markets to adapt quickly when the information flows and its transmission increase or change.[88]

Under this theory, the role of regulator is to enable and facilitate information flows among market participants to provide a fair and efficient market. In this sense, market players would have fair access to new information for decision-making, and no one would have an excessive competitive advantage over competitors.

In the blockchain space, what encumbers a fair and efficient market is the unfair access to information related to blockchain or its uses. For instance, in The DAO case, interested persons could participate in or contribute to The DAO as investors by buying tokens using virtual currency. These investors could then sell their tokens on web-based secondary market platforms in exchange for virtual currency or hold these tokens as an investment with certain voting and ownership rights. However, the problems are that not every interested person has enough information about the group that initially created The DAO, not every investor is familiar with the mechanism of how The DAO works, and not every investor could or have the incentive to properly estimate the risks and profitability of The DAO. The undue imbalance of information exists between the ones who created The DAO and other interested persons or investors.

Therefore, enabling and facilitating information is a vital goal for regulators to fulfill with regards to blockchain and its uses in the securities and depravities markets. Regulators are entrusted with a duty to monitoring the truthfulness and transparency of information. The goal of regulatory agencies under the EMH can

---

84 *Mission & Responsibilities* | U.S. COMMODITY FUTURES TRADING COMMISSION, , https://www.cftc.gov/About/MissionResponsibilities/index.htm (last visited Aug 14, 2019).

85 Eugene F. Fama, *Efficient Capital Markets: A Review of Theory and Empirical Work*, 25 J. FINANCE 383 (1970).

86 PABLO SANZ BAYÓN & LUIS GARVÍA VEGA, *An Outlook on the Role of Finance Regulation under the Fourth Industrial Revolution* (2018), https://papers.ssrn.com/abstract=3362912 (last visited Aug 10, 2019).

87 Robert J. Shiller, *From Efficient Markets Theory to Behavioral Finance*, 17 J. ECON. PERSPECT. 83– 104 (2003).

88 SANZ BAYÓN AND VEGA, *supra* note 82.

explain why the SEC enforced The DAO action that identified token offering as securities offerings. The purpose is to have similar organizations with similar intentions register with the SEC and meet the disclosure requirements, further providing transparency of information to investors. With such information, investors could better evaluate the risk associated with that blockchain project and make a proper investment decision.

2. Consumer and Investor Protection

In investment markets (i.e., securities, debilities, futures, and options markets), market manipulation, insider trading, and other frauds consistently place investors, especially individual investors, in a very vulnerable place. Many financial products allow for too much leverage, which is disclosed in a difficult-to-understand way, leaving consumers unprotected. These situations also exist in markets where blockchain gets involved, which could be even more severe than general investment markets. The severity comes from the unreasonable hype of crypto investments, the general public's the lack of knowledge of blockchain, blockchain companies' lack of investor or consumer protection mechanism, and the absence of proper regulation or rules to follow.

As the regulators or supervisors of investment or consumer markets, their goals of course are to protect investors or consumers from such dangers and maintain a sound market for all investors and consumers. Protecting investors and consumers has long been the call-in various fields, such as banking, housing, and financial products like credit cards and mortgages. Before the CFPB, responsibility for investor or consumer protection is divided between a number of federal regulatory agencies, each with different jurisdictions and missions. Therefore, the demand for an independent consumer protection agency is increasing, because consumer protection is a critical foundation for the financial system.[89] It gives the public confidence that financial markets are fair and enables policy makers and regulators to maintain stability in regulation.[90]

Having consumer protection when blockchain and its applications become an investment project or financial product like the use of cryptocurrency in the payment system can also give the public confidence. The novelty of blockchain makes it even more necessary to have such confidence. The public confidence in policymakers, regulators, the stable regulation, and a fair market can promote growth, efficiency, and innovation over the long term. That's the reason policymakers and regulators are endeavoring to place a high value on protecting consumers or investors and treating them fairly. Having an agency (i.e., the CFPB) devoted to consumer protection does not entail more regulation, but better regulation.[91]

Referring to the missions of these regulatory agencies, investor and consumer

---

89 Financial Regulation: Law and Policy (University Casebook Series): Michael S. Barr, Howell E. Jackson, Margaret E. Tahyar: 9781634592956: Amazon.com: Gateway, *supra* note 77. At 562

90 *Id.*

91 *Id.*

protection has been deeply rooted in the regulatory culture. The SEC was created with a three-part mission: 1) to protect investors; 2) to maintain fair, orderly, and efficient markets; and 3) to facilitate capital formation. [92] The CFPB protects consumers from unfair, deceptive, or abusive practices and takes action against companies that break the law.[93] The mission of CFTC is to foster open, transparent, competitive, and financially sound markets with an aim to protect market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices related to derivatives and other products that are subject to the Commodity Exchange Act.[94]

Guided by these missions and the roles of agencies designated by law, these regulatory agencies fulfill their responsibilities by issuing policies and regulations, offering education to investors and consumers, and taking enforcement actions. For example, when instant payment systems left consumers vulnerable to old and new fraudulent schemes, the FTC established its very own Blockchain Working Group to address these issues. [95] Besides, the FTC also took enforcement action against fraudsters on "chain referral schemes," unveiling how fraudsters' were dressing up old schemes with cryptocurrencies.[96]

In dealing with these obstacles, regulators have been engaging closely with investors or consumers, who are directly affected by the blockchain's involvement in the financial or investment markets. Regulators also work with innovators, developers, and entrepreneurs to get educated in this space in response to regulatory challenges. For example, the SEC established FinHub, the CFTC initiated LabCFTC, the CFPB proposed regulatory sandbox, and FTC created a Blockchain Working Group. In addition to constant consultant and research, regulators further take enforcement actions, such as in the DAO case, identifying some ICOs as securities offerings, and the Coinflip case, naming bitcoin as commodity to clear regulatory ambiguities. Such actions have been demonstrating work towards the objectives of protecting investors or consumers and fostering a sound market for them.

However, innumerable challenges inevitably slow down the accomplishment of protecting investors and consumes. For every regulator and each regulatory question, there exists a set of definitions that define the regulatory perimeter. Activities falling within that regulatory perimeter are subject to that regulatory regime, while activities outside the perimeter are not subject to that regulatory regime. In dealing with blockchain issues, especially with the extensive potential use for and relative newness of blockchain technology, regulators found it challenging to decisively conclude which agencies should oversee any specific blockchain activity. In large part, this confusion can be attributed to a lack of well-defined scope

---

92 The Role of the SEC | Investor.gov, *supra* note 79.

93 The Bureau, , CONSUMER FINANCIAL PROTECTION BUREAU , https://www.consumerfinance.gov/about-us/the-bureau/ (last visited Aug 14, 2019).

94 Mission & Responsibilities | U.S. COMMODITY FUTURES TRADING COMMISSION, *supra* note 80.

95 It's time for a FTC Blockchain Working Group, *supra* note 49.

96 FTC Shuts Down Promoters of Deceptive Cryptocurrency Schemes, *supra* note 47.

of regulatory authority in the blockchain space. In addition, given the diversity of blockchain activities, multiple agencies can be implicated both in their regulations and enforcement capabilities. Moreover, definitions vary between agencies, particularly with regard to virtual currency. The CFTC defines it as commodities, the SEC maintains they are securities, and the IRS asserts digital currency is property, while FinCEN enforced currency rules. For more details on how each agency defines blockchain technology and virtual currency, please refer to Section 1.

In addition to the ambiguity of the regulatory parameter, difficulties also exist within the scope of a certain perimeter. For example, the issuance of cryptocurrencies could be seen as a securities offering under federal securities law. To avoid the SEC's oversight, the cryptocurrency market has come up with various concepts, such as ICOs, Initial Exchange Offerings (IEOs), and Securities Token Offerings (STOs), which also raise many regulatory issues for regulators. Just as the SEC commissioner stated, "blockchain-based networks offer a new way of coordinating human action that does not fit as neatly within our securities framework." Second, the technical aspects of the technology itself increase the complexity for regulation or supervision. Regulators may not have the expertise to understand technical aspects well enough to regulate or supervise the industry. These obstacles hinder regulators from fulfilling their responsibilities to protect investors and consumers in the blockchain market.

3. Criminal Enforcement

As alluded to in the previous section, to reach the objectives of maintaining a fair and efficient market, and protecting customers and investors, it is necessary for regulatory bodies to use their law enforcement authorities. Therefore, much of the work done by regulatory bodies such as the SEC, the CFTC, and the FTC is to deter criminal acts, as well as to enforce criminal sanctions for those who break the laws under their specific jurisdictions. For instance, the SEC is involved in criminal securities fraud investigations when companies illegally use ICOs to raise capital by selling a new virtual currency to investors.

Other law enforcement agencies, such as FinCEN, the FBI, and the DOJ's Criminal Division, attempt to enforce criminal laws in general. While blockchain actions are not intrinsically criminal according to U.S. law, there are law enforcement investigations that focus on traditional criminal activity that is enabled by the use of virtual currencies and blockchain, including corruption, counter-terrorist financing, and suspected money laundering.

Take FinCEN, one of the major law enforcement agencies in the cryptocurrency space and the first one to release regulations and give guidance in regard to cryptocurrency, as an example. FinCEN has been continuously implementing, administering, and enforcing compliance with the BSA and associated regulations. FinCEN has attempted to frame blockchain through the lens of the same regulatory framework as traditional banks and financial institutions. Using the BSA (31 U.S.C. §§ 5311-5332), FinCEN has noted that any organization or individual in the technology sector that enables transactions in virtual currency or tokens may

constitute a money services business (MSB). These regulations make it clear that FinCEN's intentions are to enforce the same anti-money laundering (AML) requirements that are in effect with any other conventional MSB and money transmitters. Therefore, FinCEN requires that any MSB, including those using blockchain technology, register with FinCEN, acquire an AML compliance policy that allows for information to be collected, be assigned a compliance officer who will oversee transactions and report suspicious activities, and obey certain record-keeping requirements. All of these conditions align organizations that use blockchain technology in conjunction with virtual or hard currency, with every other U.S. financial institution.

Given the difficulties experienced by law enforcement in the cryptocurrency space—cryptocurrencies' anonymity, ability to cross borders in the fraction of a second, and the need for cross-jurisdictional collaboration—FinCEN's seeking collaboration also reflects its goal to investigate and prosecute criminals. FinCEN partners with law enforcement at all levels of governments, as well as financial institutions, in search of information on cryptocurrency transactions. Since late 2014, it has launched a collaboration with the IRS to examine more currency exchangers and administrators across the U.S. "In that time, more than one-third of all registered virtual currency money transmitters in the United States have been examined, including numerous trading platforms, foreign-located exchangers, virtual currency kiosk companies, individual peer-to-peer exchangers, and five of the 20 largest exchanges by volume. Our goal is to ensure that virtual currency exchangers and administrators are subject to the same routine compliance examinations for AML as any other financial institution."[97]

In addition to FinCEN, other law enforcement agencies have also enacted specific rules and regulations to deter and enforce criminal acts. The FBI and the Criminal Division under the DOJ, and DHS, can investigate any blockchain actions that may violate criminal law. Just as Mythili Raman, acting assistant attorney general at Criminal Division of the DOJ, testified before the Senate, the primary law enforcement interests of the DOJ are: "1) deterring and prosecuting criminals using virtual currency systems to move or hide money that is used to facilitate, or is derived from, criminal or terrorist acts, i.e., money laundering; and 2) investigating and prosecuting those virtual currency services that themselves violate laws aimed at illegal money transmission and money laundering."[98] In 2017, the FBI, DHS, and the DOJ publicized added measures to fight cyber threats, including the use of blockchain technology to facilitate anonymity in criminal enterprises.

---

97 Testimony of Thomas P. Ott, Associate Director, Enforcement Division, before the House Committee on Financial Services | FinCEN.gov, , https://www.fincen.gov/news/testimony/testimony- thomas-p-ott-associate-director-enforcement-division-house-committee (last visited Aug 20, 2019). 98 STATEMENT OF MYTHILI RAMAN BEFORE THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE FOR A HEARING ENTITLED "BEYOND THE SILK ROAD: POTENTIAL RISKS, THREATS AND PROMISES OF VIRTUAL CURRENCIES", *supra* note 55.

4. Technology Innovation

Technology innovation is a unique consideration when financial regulators craft blockchain regulation because of blockchain's technical nature and unveiled potential in the finance sector. Overregulation could stifle innovation in the financial industry, while no regulation could easily place the industry in risk. Regulators in the financial sector position technology innovation as their regulatory objective because they understand the significance of innovation and value the great potential that blockchain could generate in the financial sector. Under this regulatory objective, they further promote regulation-friendly innovation (i.e., innovation that takes account of proper regulation), not innovation with the intent to replace regulation.

At the very outset, regulators have been well aware of the importance of blockchain innovation in the financial sector. CFTC Commissioner J. Christopher Giancarlo recognized that blockchain may revolutionized the world of finance and "it will have profound implications for global financial markets by increasing settlement efficiency and speed, linking recordkeeping networks, reducing transaction costs and increasing market assess. It will broadly impact financial markets in payments, banking, securities settlement, title recording, cyber security, and trade reporting and analysis."[99] He cited one study that estimated that "DLT could eventually allow financial institutions to save as much as $20 billion by 2022 in infrastructure and operational costs each year." [100] Another study he cited reportedly estimated that "blockchain could cut trading settlement costs by a third, or
$16 billion a year, and cut capital requirements by $120 billion."[101] Therefore, he claimed "moving from systems-of-record at the level of a firm to an authoritative system-of-record at the level of a market is an enormous opportunity to improve existing market infrastructure."[102] He further proposed a "Do No Harm" regulatory approach to encourage blockchain investment and innovation.[103]

With an understanding of blockchain's importance, regulators also recognize the challenges it brings. SEC Commissioner Hester M. Peirce admitted that "[i]nnovation is always a challenge for regulators. We are used to the way things have been done. Our rules have grown up in response to past technologies. Figuring out

---

99 Special Address of CFTC Commissioner J. Christopher Giancarlo Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium | U.S. COMMODITY FUTURES TRADING COMMISSION, *supra* note 38.

100 THE FINTECH 2.0 PAPER: REBOOTING FINANCIAL SERIVCES, , http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf (last visited Aug 13, 2019).

101 Telis Demos, *Bitcoin's Blockchain Technology Proves Itself in Wall Street Test*, WALL STREET JOURNAL, April 7, 2016, https://www.wsj.com/articles/bitcoins-blockchain-technology-proves-itself-in-wall-street-test-1460021421 (last visited Aug 13, 2019).

102 Remarks of Chairman J. Christopher Giancarlo at the 4th Annual DC Blockchain Summit | U.S. COMMODITY FUTURES TRADING COMMISSION, *supra* note 35.

103 Special Address of CFTC Commissioner J. Christopher Giancarlo Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium | U.S. COMMODITY FUTURES TRADING COMMISSION, *supra* note 38. see also Remarks of Chairman J. Christopher Giancarlo at the 4th Annual DC Blockchain Summit | U.S. COMMODITY FUTURES TRADING COMMISSION, *supra* note 35.

whether and how they apply to new ideas is difficult."[104] She pointed out the biggest challenges in regulating the blockchain industry is its decentralization, which requires that regulators rethink their approach. [105] Regulators must follow innovation to proceed, even as they put in reasonable safeguards and watch for unanticipated consequences, because technological process in the financial industry offers a mix of hope, promise, and risk. The SEC regulates an industry that is a key gatekeeper for the wellbeing of the rest of the economy.

The commissioners' speeches and attitudes further imply that they not only recognize the importance and challenges of blockchain innovation, but also emphasize the need for regulators in the markets. When blockchain encounters

---

104 SEC.gov | Beaches and Bitcoin: Remarks before the Medici Conference, , https://www.sec.gov/news/speech/speech-peirce-050218 (last visited Aug 13, 2019). *accord* Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 360 (2016); Shawn Bayern, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 WASH. & LEE L. REV. ONLINE 22, 23 (2014); Jerry Brito, Houman Shadab & Andrea Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144, 146 (2014); Chris Brummer & Yesha Yadav, *Fintech and the Innovation Trilemma*, GEO. L.J. (forthcoming 2018) (manuscript at 2), https://ssrn.com/abstract=3054770 [https://perma.cc/AMN6-MX9E]; Mark Edwin Burge, *Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law*, 67 HASTINGS L.J. 1493, 1495 (2016); Omri Marian, *A Conceptual Framework for the Regulation of Cryptocurrencies*, 82 U. CHI. L. REV. ONLINE 53, 57 (2015); Hossein Nabilou & André Prüm, *Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies*, J. FIN. REG. (forthcoming) (manuscript at 2), https://ssrn.com/abstract=3121918 [https://perma.cc/6WY6-JWYV]; Seth C. Oranburg, *Hyperfunding: Regulating Financial Innovations*, 89 U. COLO. L. REV. 1033, 1034 (2018); Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191, 193 (2016); Carla L. Reyes, *Conceptualizing Cryptolaw*, 96 NEB. L. REV. 384, 399 (2017); Usha Rodrigues, *Law and the Blockchain*, 104 IOWA L. REV. (forthcoming 2018) (manuscript at 50), https://ssrn.com/abstract=3127782 [https://perma.cc/LX3C-2J64]; Scott Shackelford & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, 19 YALE J. L. & TECH. 335, 366 (2017); Anton Badev & Matthew Chen, *Bitcoin: Technical Background and Data Analysis* (Fin. Econ. Discussion Series, Working Paper No. 2014-104, 2014), https://ssrn.com/abstract=2544331 [https://perma.cc/85DV-SME3] John Michael Grant, Is Bitcoin Money?: Implications for Bitcoin Derivatives Regulation and Security Interest Treatment of Bitcoins Under Article 9 of the Uniform Commercial Code 14–15 (Dec. 17, 2014) (unpublished note), https://ssrn.com/abstract=2619457 [https://perma.cc/W7R4-CRMB]; Saman Jafari, Tien Vo-Huu, Bahruz Jabiyev, Alejandro Mera & Reza Mirzazade farkhani, Cryptocurrency: A Challenge to Legal System 4 (May 2, 2018) (unpublished manuscript), https://ssrn.com/abstract=3172489 [https://perma.cc/D36Q-XVB7]; Robert Donald Leonhard, Corporate Governance on Ethereum's Blockchain 20 (May 30, 2017) (unpublished manuscript), https://ssrn.com/abstract=2977522 [https://perma.cc/Y6K4-V5X9]; Gabriel J. Michael, Anarchy and Property Rights in the Virtual World: How Disruptive Technologies Undermine the State and Ensure that the Virtual World Remains a 'Wild West' 21 (Mar. 1, 2013) (unpublished manuscript), https://ssrn.com/abstract=2233374 [https://perma.cc/6XW3-4XK3]; Jeanne L. Schroeder, Bitcoin and the Uniform Commercial Code 4 (Aug. 22, 2015) (unpublished manuscript), https://ssrn.com/abstract=2649441 [https://perma.cc/5PDR-XX2L]; David Yermack, Is Bitcoin a Real Currency? An Economic Appraisal (Apr. 1, 2014) (unpublished manuscript), https://ssrn.com/abstract=2361599 [https://perma.cc/ZF6G-WWQX].

105 SEC.gov | Regulation: A View from Inside the Machine, *supra* note 24.

finance, some see regulation as being against financial and technology innovation because regulation could create barriers to entry and protect the status quo of existing players.[106] Others see regulation as a necessary guidance. Along with the latter group, U.S. regulators seek to engage in innovation with their regulatory power. Just as a metaphor Hester Pierce has made in her speech, regulators are like safeguards on the beach—they are not sitting with sandcastle builders monitoring their every design decision, but spot dangerous activities and intervene with a blow of the whistle or a direct action.[107]

With the attitude of engaging, regulators have been actively participating in the blockchain space like "lifeguards." For example, starting in 2013, the SEC started to issue investor alerts about Ponzi Schemes incorporating cryptocurrencies. [108] Subsequently, the SEC has put forth many statements and guideposts to help markets and investors, including by releasing investor bulletins on ICOs, investigative reports on what makes an ICO a security offering, statements by Chairman Clayton and other commissioners on these issues, and joint statement with CFTC about enforcement of cryptocurrency-related products.[109]The SEC also has spoken indirectly through a number of enforcement actions, which necessarily involved finding that the token offerings at issue were securities offerings.

The CFTC has been taking part in the blockchain industry closely as well. Since the "Do No Harm" approach was proposed, the CFTC's Technology Advisory Committee established a Subcommittee on Distributed Ledger Technology and Virtual Currencies. Meanwhile, their own Lab CFTC has produced a "Primer on Smart Contracts" addressing blockchain. The CFTC also filed a series of enforcement actions against perpetrators of fraud and market abuse involving cryptocurrencies and settled several cases that addressed and confirmed that bitcoin is a commodity and under CFTC's supervision. The CFTC took additional steps to craft a modern regulatory approach, which is predicated on four key elements: 1) adopting an exponential growth mindset, 2) creating an internal Fintech stakeholder, 3) becoming a quantitative regulator, and 4) embracing market-based solutions.[110]

In addition, the CFPB introduced a regulatory sandbox to support blockchain and other financial technology innovation, with the intent to facilitate the

---

106 Financial Regulation: Law and Policy (University Casebook Series): Michael S. Barr, Howell E. Jackson, Margaret E. Tahyar: 9781634592956: Amazon.com: Gateway, *supra* note 77. at 5

107 SEC.gov | Beaches and Bitcoin: Remarks before the Medici Conference, *supra* note 100.

108 SEC OFFICE OF INVESTOR EDUCATION AND ADVOCACY, *Investor ALert Ponzi schemes Using virtual Currencies*, https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf (last visited Aug 13, 2019).

109 LAWRENCE J. TRAUTMAN, *Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace* (2018), https://papers.ssrn.com/abstract=3182867 (last visited Aug 10, 2019). See also *Crapo Statement at Hearing on Virtual Currency: Hearing Before the S. Comm. on Banking, Housing & Urban Affairs*, 115th Cong. (2018) (statement of Sen. Mike Crapo, Chairman, S. Comm. on Banking, Housing, and Urban Affairs). *Investor Alert: Bitcoin and Other Virtual Currency-Related Investments*, INVESTOR.GOV (May 7, 2014), https://www.investor.gov/additional-resources/news- alerts/alerts-bulletins/investor-alert-bitcoin-other-virtual-currency [https://perma.cc/U3HZ-TR9X].

110 Remarks of Chairman J. Christopher Giancarlo at the 4th Annual DC Blockchain Summit | U.S. COMMODITY FUTURES TRADING COMMISSION, *supra* note 35.

advancement of the consumer finance marketplace. The motivating notion behind a regulatory sandbox is to place the regulator and innovator in the sandbox.[111] "Not only is [regulator] right there to make sure that nobody gets hurt, but she has a front- row seat on the innovative process. She sits at the entrepreneur's shoulder as he thinks through how to address structural and aesthetic weaknesses in his sandcastle."[112]

All these speeches and actions indicate regulators' understanding of the importance and challenges of blockchain innovation, as well their determination to engage in technology innovation with regulatory power. The purpose is to pursue technology innovation, especially blockchain innovation, to unlock the benefits of blockchain in the financial sector with their regulatory power.

C. Have These Objectives Been Fulfilled?

Assessing if objectives have been fulfilled is the process that regulators can understand the extent to which the regulation is achieving its objectives, and whether the implementation is "on track." This is the preliminary and necessary step to carry out the next step of rulemaking, such as changing certain rules based on the impact assessed or continuing certain rule enforcement to maximize its positive impacts.

When evaluating whether the objectives have been fulfilled, particular attention should be paid to impacts that these policies and regulations have generated. Following the order of regulatory objectives, this article evaluates impacts from four dimensions: impacts on the market in general, investor and consumer protection, criminal enforcement, and technology innovation.

1. Impacts on the Market in General

As discussed in the previous session, under the theory of EMH, to achieve the goal of a fair and efficient market, regulators' role is to enable and facilitate information flows among market participants. Thus, the focus of assessing whether the objective has been fulfilled should center on the information flows among market participants. In the blockchain space, the information flows can be made possible and accelerated through regulators' support in the adoption of blockchain, and regulators' disclosure technique. These two are also be the indicators in the assessment.

Regulators' support in adopting blockchain can enable and promote information flows because blockchain itself is decentralized in nature. Decentralization means the process by which the activities of an organization, particularly those regarding planning and decision-making, are distributed or delegated away from a central, authoritative location or group. The information is not held by a central authority, but rather is distributed to a variety of individuals or groups. The situation that every individual or group can share information freely with

---

111 Playing in the Regulatory Sandbox, , NYUJLB , https://www.nyujlb.org/single-post/2018/01/08/Playing-in-the-Regulatory-Sandbox (last visited Aug 13, 2019).

112 SEC.gov | Beaches and Bitcoin: Remarks before the Medici Conference, *supra* note 100. See also Playing in the Regulatory Sandbox, *supra* note 107.

whichever recipient or with the public accelerates and minimizes information flows for exchange. This is the case in the blockchain network. "Blockchain" means "to take the postulates of the EMH to its maximum expression," and allows "all market payers in a network, at the technical level, the same degree of information, and [the ability to] assess and verify computationally all the transactions of such network."[113] In addition, blockchain technically allows "market players [to] obtain and participate in all available information and with maximum security and reliability."[114]

Additionally, data science also contributes to greater market efficiency, especially when big data and data mining are focused on business analytics.[115] In this sense, as the EMH, the market to be efficient must have a continuous, public, and secure supply of information. [116] Blockchain can meet this goal through the generation of information flows without intermediaries, but includes technological security that makes it impossible to alter or hack the data deployed on the network.[117] The function of technological security also helps fulfill regulators' role in authenticating information, such as the identity of participants and the financial state of companies in the market, which furthers market efficiency.

However, regulators do not seem to support the blockchain adoption in a very active way even if blockchain can partially help to reach the objective of maintaining a fair and efficient market by accelerating information flows. Through the study of regulators' attitudes, summarized in the first session, it is evident that regulators hold a very neutral and cautious stance regarding the adoption of blockchain. As indicated by Commissioner Peirce, there is an open mind as to the development of blockchain technology, evidenced by the delaying of drawing clear lines, thus allowing more freedom for the technology to come into its own.

In addition, regulators are still in the process of educating themselves about the potential and risks of blockchain. There is concern about what disruptive impacts blockchain could bring to the integrity of the investment markets. For example, the chairman of CFTC, Christopher Giancarlo, stated that the potential of blockchain and its impact on financial markets has been a key focus of theirs. Commissioner Brian Quintenz expressed his concerns regarding cryptocurrency futures, which include the futures contract's financial integrity and price volatility. With respect to the potential regulated individuals and groups, regulators keep educating and warning them of the risks of blockchain and associated scams and fraud, by releasing reports, alerts, and announcements. Their enforcement actions serve as an ex-post remedy to punish or settle with those who have violated law, sending a signal to the public about how they deal with certain activities subject to regulators' oversight. None of these demonstrate

---

113 SANZ BAYÓN AND VEGA, *supra* note 82. At 11; see also UK Government Chief Scientific Adviser (2016), Distributed Ledger Technology: beyond BlockChain.

114 *Id.* see also Tapscott, D. and Tapscott, A. (2016). The impact of BlockChain goes beyond Financial Services. Harvard Business Review, May.

115 *Id.* at 13

116 *Id.*

117 *Id.*

that regulators take a strong stance on supporting the adoption of blockchain.

The second indicator for the assessment is regulators' disclosure technique. Disclosure is more of a traditional method that regulators use to facilitate information flows in the market and guarantee that market participants have fair access to information for a better decision-making. The SEC, for example, outlines and enforces disclosure requirements for firms incorporated within the United States. Companies must follow the SEC's regulations to be listed on major U.S. stock exchanges. Disclosure items include those related to a company's financial condition, operating results, and management compensation.

However, disclosure in the blockchain space is inadequate, and thus the impact on information flows is limited. With respect to blockchain, the scope of the SEC's oversight mainly concentrates on cryptocurrencies and their use to raise capital. The SEC applied longstanding securities law principles to demonstrate that a particular token constituted an investment contract and therefore was a security under our federal securities laws. Securities law seems to advance information flows by requiring disclosure of blockchain companies conducting ICOs. However, the crucial fact is that no company had been registered with the SEC as of February 6, 2018. The Chairman of the SEC, Jay Clayton, testified before the Senate that, "to date, no ICOs have been registered with the SEC, and the SEC also has not approved for listing and trading any exchange-traded products (such as ETFs) holding cryptocurrencies or other assets related to cryptocurrencies."[118]

Moreover, although the SEC emphasized that the utility characteristics of a token did not prevent the token from being a security, there are still limited companies under the SEC's supervision. Those companies with cryptocurrencies that are not securities are beyond the SEC's jurisdiction. For example, a token that represents a participation interest in a book-of-the-month club may not implicate securities laws and may well be an efficient way for the club's operators to fund the future acquisition of books and facilitate the distribution of those books to token holders.[119] These sorts of companies still issue or receive tokens (i.e., their customers are still involving monetary exchange in substance with these companies). A chance exists that customers could be ripped off. In that case, the disclosure of relevant information of a company or project is from the company itself. The company has the intention of not disclosing information that would impede the company from receiving funding. Further, the company may fail to deliver promises made to the customers.

The failures to disclose and to deliver promises in some cases further prove that information flows cannot be guaranteed effectively in the market under the existing regulation. According to an empirical study that collected whitepapers and other disclosures for the 50 top-grossing ICOs of 2017, then analyzed how the

---

118 SEC.gov | Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC, , https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and- exchange-commission (last visited Aug 19, 2019).

119 SEC.gov | Statement on Cryptocurrencies and Initial Coin Offerings, , https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11#_ftn7 (last visited Jan 27, 2018).

software code controlling the projects' ICOs reflected (or failed to reflect) their disclosure, almost all issuers promise a supply restriction in their marketing documents (40 of 45, or approximately 90%).[120] However, only about two in three (29 of 45, or approximately 64%) firms audited encoded a supply restriction.[121] There are significant differences between code and contract (whitepapers) in the sample. Thus, the failures to encode promises into the codes and deliver promises mean that information flows are not satisfied.

Although regulators fail to effectively enable and accelerate information flows through the support of blockchain adoption and the disclosure technique, regulators do have some impacts on the market in general. Regulators' constant enforcement actions, to some extent, have been deterring bad actors from conducting illegal activities. This is evident through my interviews with blockchain companies, many of which have been paying close attention to compliance and regulatory issues. Consulting with lawyers and regulators, and having legal counsels do their job allow blockchain companies to avoid violating the law. Some of intended cryptocurrency issuers gave up their plans after consulting lawyers. Some investors somehow became cautious about their investments in the cryptocurrency projects because of the education from and enforcement actions taken by regulators.

2. Impacts on Investor and Consumer Protection

Lawmakers' approaches to consumer and investor protection are guided by their philosophical, political, and economic beliefs, as well as the influence of stakeholder battles at the time a policy choice is made.[122] One factor that influences policy choices is the policymakers' theoretical framework of consumer behavior (i.e., how consumer and investor protection regulations should be structured). [123] Two schools of economic thought, neoclassical and behavioral economics, held different opinions. Neoclassical economics' idea is that competitive markets—those with multiple, self-interested players on both sides, armed with relatively full information
— will generate a mix of goods and services that is superior to those that can be generated with various forms of government regulation.[124] This conclusion becomes the usual point of controversy as behavioral economics, grounded in both economics and psychology, argue that consumers and investors have imperfect rationality and

---

120 Cohney, Shaanan and Hoffman, David A. and Sklaroff, Jeremy and Wishnick, David, Coin- Operated Capitalism (2019). Columbia Law Review, Vol. 119, p. 591, 2019, U of Penn, Inst for Law & Econ Research Paper No. 18-37, Available at SSRN: https://ssrn.com/abstract=3215345 or http://dx.doi.org/10.2139/ssrn.3215345 (last visited Aug 10, 2019).

121 *Id.* at 638

122 *Financial Regulation: Law and Policy* (University Casebook Series): Michael S. Barr, Howell E. Jackson, Margaret E. Tahyar: 9781634592956: Amazon.com: Gateway, *supra* note 77.at 555

123 *Id.* at 555

124 Richard Allen Epstein, *The Neoclassical Economics of Consumer Contracts* (2007). at 804; see also *Cf.* F. A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 530 (1945) (describing issues caused by imperfect and dispersed informa- tion).

do not always make utility decisions.[125]

Under the theory of neoclassical economics, government's regulation on consumer and investor protection is justified only in non-competitive, monopolized markets, or in markets characterized by information asymmetries. In a non- competitive market, regulation should aim at preventing the creation or requiring the divestment of monopoly power; or direct product regulation can be used to protect investors and consumers by requiring terms and prices for financial products and services that would be present in a competitive market. In a market with information asymmetries, regulation should focus on mandatory disclosure of the terms of the financial products or services.

On the other hand, under the theory of behavioral economics, government regulation should "take account of the importance of framing and defaults, of the gap between information and understanding, and between intention and action, as well as of other psychological factors affecting how people behave."[126] At the same time, behaviorally informed regulation should consider not only behavioral insights of individuals, but also economic insights about markets, because "markets can be shown to systematically favor overcoming behavioral biases in some contexts, and to systematically favor exploring those biases in other contexts." Reasons why consumers fail to make utility-maximizing decisions in selecting financial products and services may vary. Some consumers may have present-biased preferences, which lead them to favor present consumption, while some consumers may have cognitive capacity to optimize their financial situation even if presented with all the information.[127] Thus, as the outcomes about the interaction between individuals with specific psychologies and firms that respond to those psychologies with specific markets may not be socially optimal, regulation could potentially be useful to address the social welfare failures.[128]

In the context of blockchain regulation, regulators seem to adopt the approach of neoclassical economics. Blockchain and its applications are more fit for a market characterized by information asymmetries. For example, when a blockchain project appears in the market seeking investment, without any doubt, the group or company that issues this project holds more information than the general public. To protect potential investors, the SEC would step in, requiring this group or company to register with the SEC to meet all the disclosure requirements, or file a Form D Notice, which offers certain exemptions, if this project is considered an investment contract under securities law.

A further question is to what extent the SEC could protect these potential investors. In fact, the scope of protection is limited. In the SEC's Electronic Data Gathering, Analysis, and Retrieval system, a total of 39 crypto- and blockchain- related companies with the words "crypto" and "blockchain" in their company names

---

125 Oren Bar-Gill, *The Behavioral Economics of Consumer Contracts*, MINN. LAW REV. 54.

126 Michael Barr, Sendhil Mullainathan & Eldar Shafir, *Behaviorally Informed Financial Services Regulation*, PUBL. (2008), https://repository.law.umich.edu/other/29.

127 John Y. Campbell et al., *Consumer Financial Protection*, 25 J. ECON. PERSPECT. 91–114 (2011).

128 Barr, Mullainathan, and Shafir, *supra* note 122.

have filed notices with the SEC since 2014: four of those companies filed from 201 to 2016, 12 filed in 2017, and 23 filed just four and a half months into 2018.[129] Hundreds of new blockchain-related companies have appeared since 2014, many of which sought or are still seeking investments. They have been reaching out to a broad spectrum of potential investors. As of mid-April of 2018, only 39 companies filed notices with the SEC, which provided limited information to the public due to the exemption rules. Many other companies do not provide sufficient information because they seek ways to avoid the SEC's oversight. For example, some companies structure their cryptocurrencies as utility tokens to get around the securities regulation. Therefore, potential investors are exposed to information asymmetry to a great extent, as hundreds of blockchain companies do not make relevant information available to the markets or are not required by law to do so.

This approach of neoclassical economics assumes that potential investors are rational and can make informed decision when they have enough information about the company issuing a project, such as the technical aspects, the functions, or even the profitability of this project. However, this is not always the case, especially in the cryptocurrency field. Investors lack either the incentive, or capability, or both, to investigate the truthfulness of the information with which they are presented. Even if a company discloses the information of a blockchain project on its whitepaper in great details, or meets the disclosure rules required by law, investors or consumers could still fail to see useful information, such as data and objective assessments, but invest in other companies because they are backed by celebrities. These cases show that investors and consumers' failures also result from imperfect rationality and not making utility-maximizing decisions. Worse, regulation to protect investors or consumers from this approach are absent in the existing blockchain regulations. Therefore, investors and consumers involved in the blockchain space are not well protected under the existing regulatory regime.

3. Impacts on Criminal Enforcement

The fulfillment of criminal enforcement would not only signal that law enforcement agencies have accomplished their missions but would also indicate their irreplaceable role in dealing with emerging technologies. To assess the impacts of the criminal enforcement in the blockchain space, three indicators—that crimes have been identified, the emergence of new types of threats and crimes, and the loss of enforcement authority—can be used to draw a fair conclusion.

First, criminal enforcement in the cryptocurrency field had made great progress in recent years. Although no exact number of how many criminals have been prosecuted and how much value of losses have been prevented in the U.S., law enforcement agencies have been making great progress in going after criminal activities. The taking down of Silk Road by the FBI in 2013 may represent law

---

129 *Rapid Increase in SEC Filings By Cryptocurrency and Blockchain Companies*, CRYPTO LAW , https://www.cryptolaw.net/blog/2018/4/24/rapid-increase-in-sec-filings-by-cryptocurrency-and- blockchain-companies (last visited Aug 18, 2019).

enforcement agencies' willingness to tackle cryptocurrency theft and the use of cryptocurrencies for illegal transactions. Since then, the scope of law enforcement has been expanding to any criminal law violation using cryptocurrencies.

For example, in 2017, the FBI shut down the largest marketplace on the darknet, AlphaBay, which operated for more than two years and had transactions exceeding $1billion in bitcoins and other digital currencies. [130] In 2019, the FBI announced the results of Operation SaboTor, a coordinated international effort targeting drug trafficking organizations operating on the darknet. [131] With the international cooperation, law enforcement agencies made 61 arrests, shut down 50 darknet accounts used for illegal activity, and seized $7 million, $4.5 million of which was in cryptocurrency. [132] In June, 2019, The DOJ charged Roger Karlsson with securities fraud, wire fraud, and money laundering via cryptocurrency, alleging that he defrauded more than 3,500 victims of more than $11 million.[133] In March 2019,
U.S. Attorney's Office announced charges against the leaders of "OneCoin," a multibillion-dollar pyramid scheme involving the sale of a fraudulent cryptocurrency.[134] In February 2019, the FBI charged Homero Joshua Garza with 21 months in prison followed by three years of supervised release.[135] Garza fraudulently drew investors to his enterprises, which sold bitcoin-mining hardware, offered shares in a virtual currency mining operation, and created and sold a virtual currency called PayCoin. He eventually resorted to Ponzi-scheme tactics to delay detection of his fraud.[136] The victims of this virtual currency scam lost more than $9 million.[137]

However, taking down these criminals also demonstrates that scams and fraud still exist in the cryptocurrency realm. Most of them are traditional crimes enabled by cryptocurrencies, such as Ponzi schemes, pyramid schemes, securities fraud, wire fraud, and money laundering. While some criminals have been punished, many more may remain undetected. Cryptocurrencies continue to reflect billions of dollars suspicious activity. FinCEN analysis indicates that virtual currency transactions

---

130 The FBI Story 2017, FEDERAL BUREAU OF INVESTIGATION , https://www.fbi.gov/file-repository/the-fbi-story-2017.pdf/view (last visited Aug 21, 2019). P 91

131 J-CODE Announces 61 Arrests in its Second Coordinated Law Enforcement Operation Targeting Opioid Trafficking on the Darknet — FBI, https://www.fbi.gov/news/pressrel/press-releases/j-code- announces-61-arrests-in-its-second-coordinated-law-enforcement-operation-targeting-opioid- trafficking-on-the-darknet (last visited Aug 21, 2019).

132 *Id.*

133 *Alleged Cryptocurrency Fraudster Arrested In Thailand, Charged In Multi-Million Dollar Investment Scheme*, (2019), https://www.justice.gov/usao-ndca/pr/alleged-cryptocurrency-fraudster- arrested-thailand-charged-multi-million-dollar (last visited Aug 21, 2019).

134 Manhattan U.S. Attorney Announces Charges Against Leaders Of "OneCoin," A Multibillion- Dollar Pyramid Scheme Involving The Sale Of A Fraudulent Cryptocurrency, (2019), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-leaders- onecoin-multibillion-dollar (last visited Aug 21, 2019).

135 *Cryptocurrency Fraud,, FEDERAL BUREAU OF INVESTIGATION* ,
https://www.fbi.gov/news/stories/cryptocurrency-fraudster-sentenced-021119 (last visited Aug 21, 2019).

136 *Id.*

137 *Id.*

include over $1 billion in ransomware extortion funds and over $1.5 billion that has been stolen through hacks of virtual currency exchangers and administrators over the between 2016 and 2018.[138] FinCEN analysis also estimates that at least $4 billion in virtual currency has moved through darknet marketplaces since 2011. [139] Many criminals and criminal activities have not been prosecuted, so users of cryptocurrencies or participants in the crypto market space are still under threat. The value of losses from crimes keeps increasing despite the fact that law enforcement agencies have made progress.

Second, bad actors have been attempting a more diverse range of crypto crimes. CipherTrace identified the top 10 trending crypto threats in 2018 happened globally: SIM swapping**,** crypto dusting, sanction evasion, next-generation crypto mixers, shadow MSBs, datacenter-scale cryptojacking, lightning network transactions, decentralized stable coins, email extortion and bomb threats, and crypto robbing ransomware. [140]

Many of these threats have occurred in the U.S. For example, a relatively new form of identity theft called SIM (Subscriber Identity Module) swapping became popular. "This form of identity theft involves transferring the victim's phone number to a SIM card held by a hacker. Once SIM swapping attackers receive the compromised phone numbers, they use them to reset passwords and break into the victims' accounts, including accounts on cryptocurrency exchanges. In early 2018, a hacker used the technique to allegedly steal $23.8 million from a wealthy investor who, incidentally, is suing AT&T for the millions in stolen loot, along with an additional $200 million in punitive damages."[141] In another instance in the fall of

---

138 Testimony of Thomas P. Ott, Associate Director, Enforcement Division, before the House Committee on Financial Services | FinCEN.gov, *supra* note 93.

139 *Id.*

140 Adam Schlabach, *Cryptocurrency Anti-Money Laundering Report – Q4 2018*, CIPHERTRACE (2019), https://ciphertrace.com/crypto-aml-report-2018q4/ (last visited Aug 7, 2019). The definitions of these ten types of crypto threats are defined by CipherTrace as follow: (1) SIM swapping: An identity theft technique that takes over a victim's mobile device to steal credentials and break into wallets or exchange accounts to steal cryptocurrency. (2) Crypto dusting: A new form of blockchain spam that erodes the recipient's reputation by sending cryptocurrency from known money mixers.
(3) Sanction evasion: Nation states that use cryptocurrencies to circumvent sanctions and that has been promoted by the Iranian and Venezuelan governments. (4) Next-generation crypto mixers: Money laundering services that promise to exchange tainted tokens for freshly mined crypto, but, in reality, cleanse cryptocurrency through exchanges. (5) Shadow money service businesses
(MSBs): Unlicensed MSBs that bank cryptocurrency without the knowledge of host financial institutions, thus exposing banks to unknown risk. (6) Datacenter-scale cryptojacking: Takeover attacks that mine for cryptocurrency at a massive scale and that have been discovered in datacenters, including AWS. (7) Lightning Network transactions: Enabling anonymous bitcoin transactions by going "off-chain" and now scaling to $2,150,000. (8) Decentralized stable coins: Stabilized tokens that can be designed for use as hard-to-trace private coins. (9) Email extortion and bomb threats: Mass-customized phishing email campaigns by cyber-extortionists using old passwords and spouse names and that demand bitcoin. Bomb threat extortion scams spiked in December. (10) Crypto robbing ransomware: New malware distributed by cyber-extortionists that empties cryptocurrency wallets and steals private keys while holding user data hostage.

141 *Id.*

2018, hackers used SIM swapping to break into CrowdMachine, a California-based cryptocurrency startup, and steal all of its reserve coins, worth a $14 million.[142]

Another new type of fraud involving shadow banking services. For instance, Fowler and Yosef are charged with Lying to banks and skirting the regulations put in place by the banking industry. [143] In this case, Fowler made numerous false and misleading statements to banks to open bank accounts that were used to receive deposits from individuals purchasing cryptocurrency, and in which Fowler and Yosef falsified electronic wire payment instructions to conceal the true nature of a voluminous cryptocurrency exchange business. Hundreds of millions of dollars flowed through the crypto companies' accounts from banks located across the globe.
U.S. Attorney Geoffrey S. Berman said: "Reginald Fowler and Ravid Yosef allegedly ran a shadow bank that processed hundreds of millions of dollars of unregulated transactions on behalf of numerous cryptocurrency exchanges. "[144]

Additionally, the tech support fraud or pornography scams require payment of cryptocurrency. In 2017, the IC3 received approximately 11,000 complaints related to tech support fraud. The claimed losses amounted to nearly $15 million, which represented an 86% increase in losses from 2016.[145] Criminals may pose as a security, customer, or technical support representative offering to resolve such issues as a compromised e-mail or bank account, or a virus on a computer, or to assist with a software license renewal. Some recent complaints involve criminals posing as technical support representatives for GPS, printer, or cable companies, or support for virtual currency exchangers. [146] In the case of pornography fraud, the fraudsters purchase personal information, such as email addresses and old passwords, then email those whose personal information they have, claiming that they have hacked into their computers' cameras and have a video of them watching pornography.[147] The scammer then threatens to release this video to families, friends, or coworkers if they don't get paid. Usually, payments should be made in some form of cryptocurrency.

Third, the loss of enforcement authority indicates that criminal enforcement is facing further difficulties. According to a report released by CipherTrace, as showed in the chart below, an increasing number of cross-border bitcoin payments have been shifting from U.S. exchanges to other countries from 2017 to 2019. An analysis of 164 billion BTC transactions revealed that "cross-border payments from

---

142 *Id.*

143 Arizona Man And Israeli Woman Charged In Connection With Providing Shadow Banking Services To Cryptocurrency Exchanges, (2019), https://www.justice.gov/usao-sdny/pr/arizona-man- and-israeli-woman-charged-connection-providing-shadow-banking-services (last visited Aug 25, 2019).

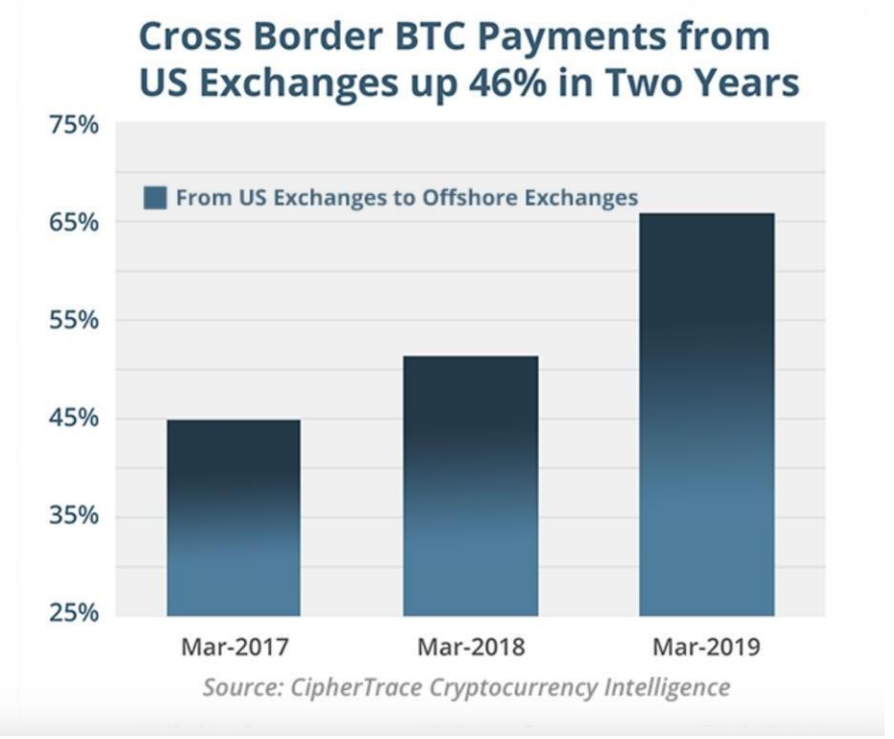
144 *Id.*

145 Internet Crime Complaint Center (IC3) | Tech Support Fraud, , https://www.ic3.gov/media/2018/180328.aspx (last visited Aug 21, 2019).

146 *Id.*

147 Oregon FBI Tech Tuesday: Building a Digital Defense Against Pornography Scams — FBI, , https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday- building-a-digital-defense-against-porn-scams (last visited Aug 25, 2019).

U.S. exchanges to offshore exchanges increased from 45% for the 12 months ending Q1 2017 to 66% in the 12 months ending Q1 2019. This is significant because according to the International Consortium of Investigative Journalists, "$8.7 trillion, 11.5 percent of the world's wealth, is hidden offshore."[148] This indicates a major hold in the currency cryptocurrency regulatory fabric with respect to cross-border payments.[149] Once an increasing numbers of these payments reach exchanges and wallets in other parts of the globe, they fall off the radar of U.S. authorities, which significantly affects U.S. criminal enforcement in the blockchain space.



4. Impacts on Technology Innovation

A problem with blockchain innovation is that blockchain implementations were sluggish because many companies involved in blockchain were at the early stage experiments, although the scope of innovation has gone beyond cryptocurrency and its related activities such as trading and storage. The market could barely see mature blockchain products or services, and widespread adoptions are still far away. It is been a decade since the first blockchain application—bitcoin— appeared in the market. The financial market is still exploring and experimenting with blockchain

---

[148] ehayse, *Q2 2018 Cryptocurrency Anti-Money Laundering Report*, CIPHERTRACE (2019), https://ciphertrace.com/q2-2018-cryptocurrency-anti-money-laundering-report/ (last visited Aug 2, 2019).
[149] *Id.* at 2

innovation. During this decade, with a goal of technology innovation in the financial sector, regulators have been issuing a number of policies and regulations that could affect blockchain's interaction with finance.

To assess whether the existing regulatory regime has achieved the objective of technology innovation, this article approaches this question from three dimensions: infrastructure for cross-border transactions, new mechanism for fundraising, and digital assets as a class. The sections that follow explain each of them, what progress has been made, and to what extent the existing blockchain regulatory regime have impacted innovation.

a. Infrastructure for Cross-border Transactions

Take IBM's World Wire as an example to explain the existing problem with the infrastructure for cross-border transactions and how blockchain could address the issue. Briefly summarized, the problem with sending an international payment through existing banking channels, which consist of clearing flow and settlement flow, is a complex process that involves several intermediaries. Going through these intermediaries requires time and money to complete. The average cost of sending payments worldwide is 7%, according to the World Bank.[150] The whole process could take two or three days (in general), or even longer to complete, depending on the regions. The high transaction fee would be a burden, especially for micropayments.

Blockchain could solve this problem "by streamlining the process and storing

> *every transaction in a secure distributed ledger. As soon as a transaction is recorded, the receiving party has access to the payment, with no middlemen, no delays, no unnecessary fees. And once a payment is entered, it can't be reversed or changed in*

the ledger, fostering greater overall accountability and security."[151] Deloitte estimates that business-to-business and person-to-person payments with blockchain result in a 40% to 80% reduction in transaction costs, and take an average of four to six seconds to finalize.[152]

What progress has been made in the U.S.? To date, many financial institutions and technology companies have been exploring the use of blockchain for building the infrastructure for cross-border payments. As of March 2019, IBM Blockchain World Wire has enabled payment locations in 72 countries, with 47 currencies and

---

150 The World Bank, *Remittance Prices worldwide*, https://remittanceprices.worldbank.org//sites/default/files/rpw_report_december_2018.pdf (last visited Aug 22, 2019).

151 Saiful Khandaker, *How Blockchain Is Transforming Cross-Border Payments*, FORBES , https://www.forbes.com/sites/forbestechcouncil/2019/03/12/how-blockchain-is-transforming-cross- border-payments/ (last visited Aug 22, 2019).

152 *Id.* see also DELOITTE, *cross-border-payments.pdf*, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/grid/cross-border-payments.pdf (last visited Aug 22, 2019).

44 banking endpoints.[153] According to IBM,

> [T]his is the first blockchain-based network that integrates payment messaging, clearing, and settlement on a single network. It reduces intermediaries and allows users to accelerate settlement time, often to seconds, by transmitting monetary value in the form of digital assets, commonly known as cryptocurrencies or "stable coins." This simplified approach improves operational efficiency and liquidity management, streamlining payment reconciliation and reducing overall transaction costs for financial institutions.[154]

Ripples, a technology company that delivers distributed technology to financial institutions, allows financial institutions to process their customers' payments anywhere in the world instantly, reliably, and cost-effectively. Banks and payment providers can also use the digital asset XRP to further reduce their costs and access new markets. Ripple already has an entire network of banks that have joined. Agreements have been signed with more than 200 banks and financial institutions, covering over 40 countries across six continents.[155]

In addition to IBM and Ripples, some other U.S. financial institutions or technology companies are also experimenting with blockchain in this space. For example, J.P. Morgan created a digital coin for payments.[156] Libra Association, a membership organization founded by Facebook's subsidiary Calibra and 27 others across payment, technology, telecommunication, venture capital, and nonprofits, proposed "a new decentralized cryptocurrency, called Libra, and a smart contract platform that together aim to create a new opportunity for responsible financial services innovation." [157] The currency and network do not yet exist, and only rudimentary experimental code has been released. Facebook announced that it plans to launch Calibra in 2020. The Stellar Development Foundation, a nonprofit organization founded in 2014, supports the development and growth of the open- source Stellar network to build a new stack for digital assets.[158] Stellar allows a user

---

153 *IBM Blockchain World Wire, a New Global Payment Network, to Support Payments and Foreign Exchange in More Than 50 Countries*, IBM NEWS ROOM (2019), https://newsroom.ibm.com/2019-03- 18-IBM-Blockchain-World-Wire-a-New-Global-Payment-Network-to-Support-Payments-and- Foreign-Exchange-in-More-Than-50-Countries (last visited Aug 22, 2019).

154 *Id.*

155 *IBM Blockchain World Wire: growing competition in payments*, FINEXTRA RESEARCH (2019), https://www.finextra.com/blogposting/17136/ibm-blockchain-world-wire-growing-competition-in- payments (last visited Aug 22, 2019). See also: RippleNet Reaches Milestone, Surpasses 200 Customers, , RIPPLE , https://www.ripple.com/ripple_press/ripplenet-reaches-milestone-surpasses- 200-customers/ (last visited Aug 22, 2019).

156 J.P. Morgan Creates Digital Coin for Payments | J.P. Morgan, , https://www.jpmorgan.com/global/news/digital-coin-payments (last visited Aug 22, 2019).

157 Libra White Paper | Blockchain, Association, Reserve, , LIBRA.ORG , https://libra.org/en-US/white- paper/ (last visited Aug 22, 2019).

158 About - Stellar Development Foundation, , https://www.stellar.org/foundation/ (last visited Aug 22, 2019).

to create a redeemable, tradable representation of any asset, reachable anywhere in the world with low costs and quick transactions.[159]

Blockchain's innovation in the infrastructure for cross-border transactions can be seen as a success. With blockchain, these new companies (Ripples and Stella), or new projects under existing companies (IBM's World Wire, JPMorgan's Morgan Coin, and Facebook's Calibra) rival Western Union or Society for Worldwide Interbank Financial Telecommunication (SWIFT), represent a new trend of cross- border transactions that allow for global reach, instant transition times, and low costs. Under the existing regulatory regime, the major regulatory burden for these companies is to satisfy AML requirements. They therefore partner with banks and other financial institutions, which have been traditionally abiding by Know Your Customer (KYC) and other AML rules, to take advantage of their competency in regulatory compliance. Even if law enforcement agencies issue new guidance on AML compliances for cryptocurrencies, it won't pose too much of an extra burden for these companies. Therefore, the existing regulatory regime does not become an obstacle for blockchain innovation in developing infrastructure for cross-border transactions.

b. New Mechanism for Capital Formation

ICOs have become a financial innovation in the fundraising space. They allow a company to raise funds from investors, and in exchange, investors receive cryptocurrencies issued by the company. These cryptocurrencies could generate value by conferring the future revenue of the company or by providing access to goods or services that the company will launch in the future. ICOs are particularly advantageous for start-ups in need of funding to start their businesses in a fast and easy way, avoiding the existing strict and over-regulated fundraising process. Compared to conventional fundraising mechanisms—seeking funds from family or friends, getting loans from banks or financial institutions, pitching venture investors, and going public, ICOs open up companies to a large investor pool, enabling startups to receive funding easier, and allowing investors, especially retail investors, access to more investment opportunities. Besides, depending on how a company structures the right of these cryptocurrencies, such as eliminating voting rights, which is normally the case in conventional shares, founders of a company can reserve control of the company while benefiting from the added value of having experienced venture capitalists on board. For investors, ICOs could provide a flexible exit mechanism. Investors could sell cryptocurrencies and liquidate easily on the secondary market. As a new type of fundraising mechanism, ICOs offer many advantages to both fundraisers and investors.

However, cryptocurrencies and the use of cryptocurrencies will gradually become heavily regulated in the U.S. Under the existing regulatory regime, the SEC

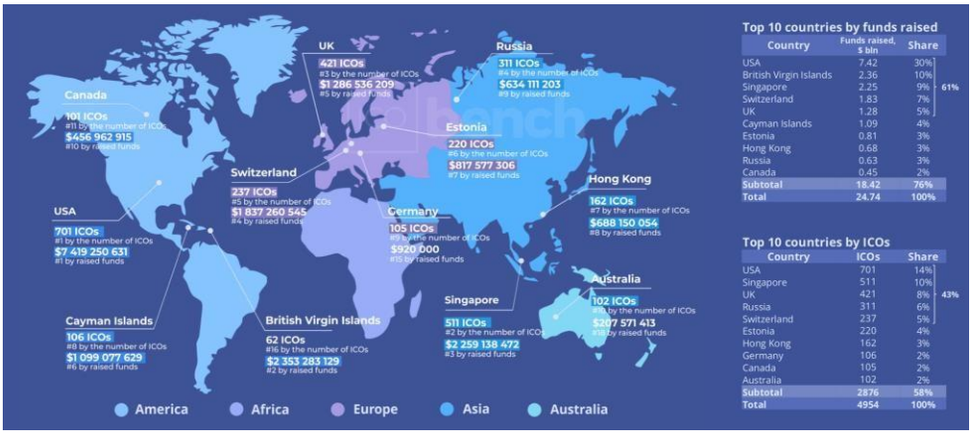
---

[159] Asset Issuance - Explainer - Stellar Development Foundation, , https://www.stellar.org/foundation (last visited Aug 22, 2019).

treats some cryptocurrencies as securities, and the issue of cryptocurrencies as securities offering. The CFTC sees bitcoin as a commodity. The IRS treats it as property subject to tax. The FTC and the CFPB focus on the consumer protection aspect of using cryptocurrencies. Law enforcement agencies—FinCEN, the FBI and the Criminal Division of the DOJ— keep close eyes on the use of cryptocurrencies for fraud and any other illegal activities. The cryptocurrency space seems no longer as free and open as it used to be. Every move of cryptocurrencies, including the use for fundraising, is likely under supervision now.

Under the existing regulatory regime, how do ICOs perform in the U.S.? According to an ICObench's report releasing top countries standing out regarding the number of ICOs launched and the number of funds raised by the end of 2018, the U.S. ranked at the top, with 701 ICOs launched and $7.42 billion funds raised. This constituted 30% of the overall market shares in the ICO space. [160]

Figure: top 10 countries by the number of ICOs launched and funds raised by the end of 2018



Source: ICObench

However, the situation has been changing since the beginning of 2019. Using the same indicators (the number of ICO launched and the number of funds raised) the U.S. raked second by the number of ICO launched in January 2019, but was not on the list by funds raised.[161] In the following months, as shown in the chart below, the

160 ICOBENCH, *ICO_Market_Quarterly_Analysis_Q1_2019.pdf*, https://icobench.com/reports/ICO_Market_Quarterly_Analysis_Q1_2019.pdf (last visited Aug 23, 2019).

161 ICOBENCH, *ICObench_ICO_Market_Analysis_January_2019.pdf*, https://icobench.com/reports/ICObench_ICO_Market_Analysis_January_2019.pdf (last visited Aug 23, 2019). See also the reports from the following months:ICOBENCH, *ICObench_ICO_Market_Analysis_February_2019.pdf*, https://icobench.com/reports/ICObench_ICO_Market_Analysis_February_2019.pdf (last visited Aug

ranking by the number of ICOs launched was between two and four, constituting 5% to 12% market shares; the raking by the number of funds raised was between three to 10, with two months (January and March) dropping out of the list, constituting 3% to 9% market shares. By the first half of 2019, in total, the U.S. still ranked top by the number of funds raised, with $7.27 billion, which constitutes 28% market shares, and by the number of ICO launched, with 749.[162] However, by the number of ICOs launched, Singapore exceeded the U.S. raking top by the most successful ICOs with the highest number of projects that had raised funds.

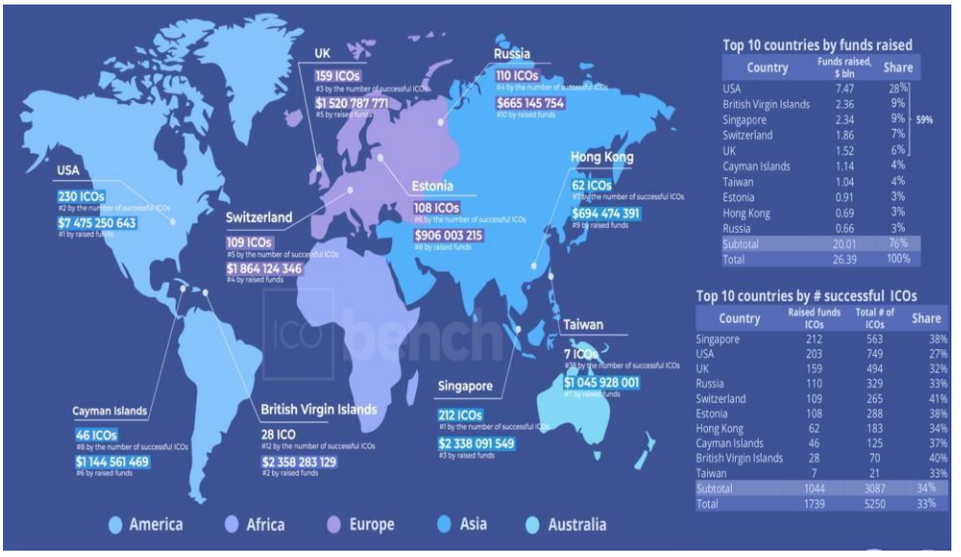
Figure: top 10 countries by the number of ICOs launched and funds raised from January to June 2019

Month, 2019	Raking by the number of ICOs launched			Raking by the number of funds raised, $		
	Ranking	The number of ICOs launched	Market shares	Ranking	The number of funds raised and market shares	Market Shares
January	2	11	9%	X	X	X
February	3	9	12%	10	4,953,413	3%
March	3	11	8%	X	X	X
April	4	8	7%	4	20,200,012	9%
May	4	6	5%	4	23,000,000	2%
June	4	9	8%	3	19,830,707	9%

Figure: top 10 countries by the number of ICOs launched and funds raised by the first half of 2019

23, 2019). ICOBENCH, *ICObench_ICO_Market_Analysis_March_2019.pdf*, https://icobench.com/reports/ICObench_ICO_Market_Analysis_March_2019.pdf (last visited Aug 23, 2019).ICOBENCH, *ICObench_ICO_Market_Analysis_April_2019.pdf*, https://icobench.com/reports/ICObench_ICO_Market_Analysis_April_2019.pdf (last visited Aug 23, 2019). ICOBENCH, *ICObench_ICO_Market_Analysis_May_2019.pdf*, https://icobench.com/reports/ICObench_ICO_Market_Analysis_May_2019.pdf (last visited Aug 23, 2019).ICOBENCH, *ICObench_ICO_Market_Analysis_June_2019.pdf*, https://icobench.com/reports/ICObench_ICO_Market_Analysis_June_2019.pdf (last visited Aug 23, 2019).

[162] ICOBENCH, *supra* note 156.



Source: ICObench

From these data, the conclusion can be draw that although the U.S. still has the base of large markets share in terms of both the number of ICOs launched and the amount raised, the U.S. ICO market witnesses a slower pace of growth starting with January 2019. It could have started earlier than that, since the data did not show the situation in 2018. While many ICOs used to be launched from the U.S., an increasing number are originating elsewhere, such as Singapore and Switzerland.

The reasons behind this decrease may vary. One reason could be the existing regulatory regime. Starting from 2017 until this year, law enforcement agencies have been increasingly explicating AML requirements in the cryptocurrency space, which could be a burden for cryptocurrency-related transactions. Regulators of securities and derivatives markets continue extending oversight over cryptocurrency and ICO markets. Some other regulators, which used to stay out of the cryptocurrency realm, have shifted gears toward overseeing the use of cryptocurrencies. Through my interviews with some entrepreneurs, they consider the U.S. is no longer a very ideal market for ICOs, due to the unclear regulatory guidance on the one hand, and strict securities regulation on the other hand. A legal counsel at a big U.S. cryptocurrency exchange complained that ICO deals have been shifting from the U.S. to Asian and European countries because of the increasing compliance burden in the U.S. Some believe that the SEC put breaks on the U.S. blockchain ecosystem "by not addressing the new phenomenon of ICOs and providing no regulatory framework for them to exist, thus stagnating U.S. blockchain development."[163]

163 Global blockchain innovation: U.S. lags, Europe and China lead, , VENTUREBEAT (2017), https://venturebeat.com/2017/04/16/global-blockchain-innovation-u-s-lags-europe-and-china-lead/ (last visited Aug 23, 2019).

c. Tokenized Assets as a Class

Deloitte claims that "the tokenization of assets is disrupting the financial industry."[164] The tokenization of assets refers to the process of issuing a blockchain token (specifically, a security token) that digitally represents a real tradable asset— in many ways similar to the traditional process of securitization.[165]Comparing to traditional assets such as equity, real estate, investment funds, real estate investment trusts and others, tokenized assets are the digital representations of these physical assets. Why not call them digital assets? A problem with digital assets is that they are easily copied. Pure digital assets lack uniqueness, which prevent them from accurately and securely representing physical assets. For example, it's easy for anyone to copy a picture online and claim the ownership. Blockchain could provide a solution because of its capacity to prevent double spending. Thus, if that picture is stored on blockchain and recorded on blockchain and comes with a unique code, it can be easily verified.

A great way to illustrate the tokenization and the benefits of tokenized assets is through the example that follows:

> Suppose there is a $200,000 apartment. Tokenization can transform this apartment into 200,000 tokens (the number is totally arbitrary; we could have issued two million tokens). Thus, each token represents a 0.0005% share of the underlying asset. Finally, we issue the token on some sort of a platform supporting smart contracts, for example on Ethereum, so that the tokens can be freely bought and sold on different exchanges. When you buy one token, you actually buy 0.0005% of the ownership in the asset. Buy 100,000 tokens and you own 50% of the assets. Buy all 200,000 tokens and you are 100% owner of the asset.[166]

In this case, a person does not need $200,000 to invest in real estate. A very modest minimum could be enough. A person also does not need to sell the whole property, worth $200,000, for an emergent need of $50,000. He could just sell 50,000 tokens to satisfy his need. Thus, A clear benefit of tokenized assets is a lower barrier to entry. Different from those high costs of investments, such as real estate or fine art, which are out of reach for many, tokenized assets are effectively accessible by retail investors and allow for investments with flexible time and amount. The lower barrier to entry opens the door to a larger pool of investors.

A second benefit of tokenized assets is that it offers greater liquidity. Compared to traditional assets, such as real estate and private equity, which are practically illiquid and should rely on certain network to find buyers and sellers, these tokens can be traded on the secondary markets easily. "This access to a broader base of traders increases the liquidity, benefiting investors who consequently have more

---

164 THE TOKENIZATION OF ASSETS IS DISRUPTING THE FINANCIAL INDUSTRY, 6.

165 *Id.*

166 George Sazandrishvili, *Asset Tokenization on Blockchain Explained in Plain English*, MEDIUM (2019), https://medium.com/coinmonks/asset-tokenization-on-blockchain-explained-in-plain-english-f4e4b5e26a6d (last visited Aug 22, 2019).

freedom and sellers because the tokens benefit from the 'liquidity premium,' thereby capturing greater value from the underlying asset."[167]

Other benefits come from the properties of blockchain from a technically point of view. For example, tokenization reduces transaction costs because transactions on blockchain reduce intermediaries. As a result, fees for middlemen and transaction time are cut down. For the same reason, transacting on blockchain also facilitates rapid settlement. Due to the nearly immutable characteristic of blockchain, tokenized assets offer transparency and traceability, which further protect investors from being ripped off.

Although tokenization of assets could offer many benefits, so many questions arise. For example, does owning 100% tokens of a property present 100% ownership in a legal sense? Does allowing retail investors to invest in certain markets provide better protection? What's the standard for tokenizing assets? Is there minimum share of ownership that can be devised? Where can people trade these tokenized assets? What are the best rules for trading these assets? Who should guard these tokens? How would it affect traditional asset management firms? All these questions require not only technical, but also regulatory and even societal, responses before tokenized assets can become reality.

The idea of tokenized assets as a class is still theoretical at this point. Under the existing regulatory regime, the biggest hurdle preventing it from becoming a reality is the lack of policy guidance and specific regulation. The only regulation that may be directly relevant to tokenization is securities law. Because the process of issuing tokens, if done through ICO or trading tokens, could be treated as a securities offering, which is subject to securities regulation. To a greater extent, many issues surrounding tokenized assets as a class cannot find an answer in existing laws. There is not even a policy environment for the evolvement of this idea. Therefore, the existing regulation regime has no direct impacts on the innovation of tokenized assets as a class, and indirectly, it slows down the innovation in this field.

Blockchain's potential in promoting innovations in the financial sector could occur in many other scenarios. For instance, along with smart contract, blockchain could be used for regulatory reporting and compliance. Because of blockchain's self-contained system of record, it could be used for risk management, loan management, accounting, and auditing. But many of these either are at theoretical discussions or early-stage experiments. Thus far, almost no mature applications or implementations in these fields take place in the U.S. Some companies may test out new applications, but it is difficult to attribute how the existing regulatory regime affect their innovations, especially when impacts of an application itself have not be spread. Thus, these topics are not covered under this session.

Overall, although technology innovation is a regulatory objective when regulators craft blockchain regulation, their true attitude towards to technology innovation, especially blockchain innovation in the financial sector, is that they don't want to stifle innovation, and at the same time, they don't want to be blamed for

---

[167] The tokenization of assets is disrupting the financial industry, *supra* note 159

promoting progressive innovation, which could result in unexpected disasters. Thus, with a somewhat open but cautious mind, regulators exercising regulatory power through policies, regulations, rules, or guidance don't lead to positive impacts on all technology innovations. While the innovation in building infrastructure for cross-border transactions may see some progresses, the innovation in establishing new mechanism for fundraising is lagging behind, and the idea of tokenized assets as a class is still at the theoretical discussion stage. Many technological, regulatory, and conception issues are waiting to be addressed before the financial industry can see greater blockchain innovation.

III. CONCLUSION

It has been a few years since the U.S. started to take regulatory actions consistently and regularly in the blockchain space. We have already witnessed a portion of the impacts of some regulatory actions meant for the blockchain industry, yet other impacts of regulatory actions may be hard to estimate. After assessing the impacts of the existing blockchain regulatory regime, it is fair to conclude that some of the objectives of the regulatory actions have been fulfilled while others have not. Specifically, this article uses four major indicators to help determine whether regulatory actions toward blockchain technology and its applications generate their intended effects.

First, under the theory of EMH, general impacts on the market should be assessed through regulators' support for the adoption of blockchain and regulators' disclosure techniques. The regulators did not seem to support blockchain adoption in an active way, and they were still in the process of educating themselves about its potential and risks. Disclosure in the blockchain space was inadequate, and thus its impact on information flows was limited. The failures to disclose and deliver promises in some cases further proved that information flows cannot be effectively guaranteed in the market under the existing regulations. However, regulators did have some impacts on the market in general. Their constant enforcement actions, to some extent, have deterred bad actors from conducting illegal activities. Their constant issuing of statements, investor alerts, and legal explanations gave the market some clarity with respect to their attitudes and acceptable behaviors in the market.

Second, to protect investors and consumers, regulators focused on mandatory disclosure. However, the result was unsatisfactory. The scope of protection was limited because the consumers and investors were not always rational and could not always make informed decisions in the blockchain space. They lacked either the incentive or capability (or both) to investigate the truthfulness of the information they were presented.

Third, criminal enforcement in the field of cryptocurrency has made great progress in recent years. However, constantly taking down these criminals has also demonstrated that scams and fraud still exist in the cryptocurrency realm. Bad actors have been attempting a more diverse range of crypto crimes. Criminal enforcement faced further difficulties when an increasing number of cross-border bitcoin

payments shifted from U.S. exchanges to other countries.

Fourth, in terms of technological innovation, blockchain's innovation in the infrastructure for cross-border transactions can be seen as a success. However, ICOs—which have become a financial innovation in the fundraising space—will not be widely adopted in the near future because they will gradually become heavily regulated in the U.S. In addition, although Deloitte claimed that the tokenization of assets was disrupting the financial industry, it also raised many questions for the industry and regulators. The idea of tokenized assets as a class was still theoretical at that point.

Therefore, for the future rulemaking or adjustment of the existing regulatory regime, regulators should engage in the blockchain space in a more active manner and consider alternative disclosure techniques to foster information flows and protect consumers and investors as well as better organize the blockchain market. The existing criminal enforcement mechanism regarding the illegal use of blockchain is effective, but law enforcement officials should continue studying and tackling novel, unceasing crimes in the name of blockchain and strengthen international cooperation due to the borderless nature of blockchain technology. Additionally, future rulemaking should always take technology innovation into account and be careful not to stifle innovation while crafting new rules, especially in terms of innovative ideas that are still in conceptual or theoretical phases, such as the tokenization of assets.