American University Law Review

Volume 68 | Issue 1 Article 2

2018

Crypto Securities: On the Risks of Investments in Blockchain-Based Assets and the Dilemmas of Securities Regulation

Schlomit Azgad-Tromer
Columbia Law School

Crypto Securities: On the Risks of Investments in Blockchain-Based Assets and the Dilemmas of Securities Regulation

CRYPTO SECURITIES: ON THE RISKS OF INVESTMENTS IN BLOCKCHAIN-BASED ASSETS AND THE DILEMMAS OF SECURITIES REGULATION

SHLOMIT AZGAD-TROMER*

Recent declarations and investigations by the Securities and Exchange Commission suggest that blockchain-based assets are potentially subject to regulation as securities under the Securities Act. This Article presents a systematic analysis of the risks and embedded costs of investments in blockchain-based assets and assesses their potential regulation as securities.

This Article offers a comprehensive account of the pertinent properties of blockchain-based assets, the technology of the blockchain, the markets available for their trade, and their varied underlying sources of value. It identifies unique costs and risk factors inherent to the blockchain technology, and examines whether securities laws can potentially add value and protect investors from these unique risks. Identified costs and risks factors include controlling costs prevalent even in decentralized ledgers, monitoring costs that vary according to the costs of automatic verification, technology risks rooted in the vulnerability of the blockchain to bugs in its software, and systemic risks embedded in limited transparency and contractual rigidity of the blockchain-based investment contract.

This Article examines these unique costs and risk factors and assesses their normative implications for securities regulation of blockchain-based assets. With current efforts by regulatory authorities to designate blockchain-based assets as securities, a coherent approach is presented based on the type of the offering, investors' profile, and the technical and legal contours of the blockchain-based

---

* Associate Research Scholar, *Columbia Law School.* Thanks for helpful comments and conversations go to Mike Burstein, Mirit Eyal-Cohen, Geeyoung Min, and to participants of the Law and Entrepreneurship Retreat at Alabama Law School, the Roundtable discussion at Fordham Center on Law and Information Policy, and the Associates Seminar at Columbia Law School. Special thanks to Eran Tromer, for decades of thought-provoking and fruitful conversations, including the inspiration for this paper.

asset under assessment. The analysis proposes that securities regulators should target the identified costs and risk factors and assess the potential of securities regulation to protect investors, based on a structural and technical assessment of the blockchain-based asset under consideration and as balanced against the costs of securities regulation. The proposed approach is illustrated by examining several blockchain-based assets, including Bitcoin, Tezos, and Filecoin.

TABLE OF CONTENTS

INTRODUCTION

The technology underlying blockchains has revolutionized financing of entrepreneurial businesses.[1] According to a report by *Forbes*, investments in blockchain platforms exceeded venture capital investments in the first half of 2017, attracting the participation of banks, big tech firms, and startups.[2] With the aggregate global crypto market capitalization exceeding $300 billion, investments in blockchain offerings have become the hottest trend in contemporary finance.[3]

Recent declarations and investigations by the United States Securities and Exchange Commission (SEC) infer that blockchain-based assets are subject to regulation as securities,[4] suggesting that token and cryptocurrency offerings without registration are violating the Securities Act,[5] thus marking a critical juncture for the blockchain

1. *See* Alex Tapscott & Don Tapscott, *How Blockchain is Changing Finance*, HARV. BUS. REV. (Mar. 1, 2017), https://hbr.org/2017/03/how-blockchain-is-changing-finance (identifying blockchain as a solution for the inefficiencies in the financial system).

2. *See* Chance Barnett, *Inside the Meteoric Rise of ICOs*, FORBES (Sept. 23, 2017, 1:21 AM), https://www.forbes.com/sites/chancebarnett/2017/09/23/inside-the-meteoric-rise-of-icos ("Initial Coin Offerings ("ICOs") have quickly grown to account for more startup funding in blockchain-based companies than all of Venture Capital.").

3. *See* Nate Nead, *Cryptocurrency & Blockchain Market Capitalization, Opportunities and Risks*, INV. BANK, https://investmentbank.com/crypto-market-cap (last visited Oct. 17, 2018) (noting the global crypto market cap, the rise of the industry, and its significance in monetary policy).

4. In July 2017, the SEC published a report of an investigation pursuant to § 21(a) of the Securities Exchange Act of 1934 regarding an offering of the blockchain proposed by the Decentralized Autonomous Organization (DAO). Report of Investigation Pursuant to § 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207, at 1–2 (July 25, 2017). The DAO report determined that in this case, tokens offered in a blockchain were considered securities under the Securities Act of 1933 and the Securities Exchange Act of 1934. *Id.* at 1.

5. 15 U.S.C. § 77a (2012).

industry and its regulation.[6] According to the Securities Act, investment contracts whereby a person invests money in a common enterprise and is led to expect profits solely from the efforts of others are considered securities.[7] Securities afford investors broad protection and impose exhaustive requirements on their offerors, including, but not limited to, mandatory disclosure.[8] Different transactional approaches were suggested

---

6. In December 2017, SEC Chairman Jay Clayton made a public declaration regarding the blockchain "buzz" in financial markets, raising concerns about the industry's rapid growth. Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11 (noting that amidst rapid growth "[a] number of concerns have been raised regarding the cryptocurrency and ICO markets"). In January 2018, Chairman Clayton addressed the potential regulation of ICOs as securities in his opening remarks at the Securities Regulation Institute, stating that "[t]he SEC is undertaking significant efforts to educate the public that unregistered securities investments offered by unregistered promoters, with no securities lawyers or accountants on the scene, are, in a word, dangerous." Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, Opening Remarks at the Securities Regulation Institute (Jan. 22, 2018). In an op-ed published in January 2018, both the chairman of the SEC and the chairman of the Commodity and Futures Trading Commission voiced concern about the blockchain industry and expressed a commitment to addressing this emerging market. *See* Jay Clayton & J. Christopher Giancarlo, *Regulators Are Looking at Cryptocurrency*, WALL ST. J. (Jan. 24, 2018, 6:26 PM), https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363 (expressing concern that cryptocurrencies largely operate outside of the existing regulatory sphere and noting "[t]he SEC is devoting a significant portion of its resources to the ICO market").

In November 2017, Stanford professor and former SEC commissioner Joseph Grundfest told the *New York Times* that "ICOs represent the most pervasive, open and notorious violation of securities laws since the Code of Hammurabi." Nathaniel Popper, *Initial Coin Offerings Horrify a Former S.E.C. Regulator*, N.Y. TIMES (Nov. 26, 2017), https://www.nytimes.com/2017/11/26/business/initial-coin-offering-critic.html.

On November 1, 2017, the SEC announced that endorsement by "[c]elebrities and others . . . using social media networks to encourage the public to purchase stocks and other investments . . . may be unlawful if they do not disclose the nature, source, and amount of any compensation paid . . . by the company in exchange for the endorsement." SEC Division of Enforcement & SEC Off. of Compliance Inspections & Examinations, *SEC Statement Urging Caution Around Celebrity Backed ICOs*, U.S. SEC. & EXCH. COMM'N (Nov. 1, 2017), https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos; *see also* Hester M. Pierce, Comm'r, SEC, Beaches and Bitcoin: Remarks Before the Medici Conference (May 2, 2018) (noting the regulatory regime imposed on tokens or coins used in ICOs will shape the industry).

7. SEC v. W. J. Howey Co., 328 U.S. 293, 298–99 (1946).

8. *See id.* at 298 (stating the term "investment contract" originally implied that a level of protection was granted to investors); Frank H. Easterbrook & Daniel R. Fischel, *Mandatory Disclosure and the Protection of Investors*, 70 VA. L. REV. 669, 680 (1984) (explaining the limitations on and many requirements of firms resulting from mandatory disclosure rules in the securities industry). *See generally* JAMES D. COX ET AL.,

to hedge the regulatory uncertainty in the blockchain industry due to the SEC's declarations.[9] But why should blockchain-based assets be considered securities to begin with?

This Article proposes a systematic analysis of this question utilizing a thorough analysis of the core costs and risk factors embedded in blockchain-based investments. This Article's central claim is that blockchain-based assets have heterogeneous technical characteristics and transactional structures. Therefore, the applicability of securities laws to blockchain-based asset offerings requires evaluating the risks underlying the investment—whether investors can be left to fend for themselves given their financial profile and the nature of such risks, and whether securities laws can potentially mitigate these embedded costs and risk factors and add value to investors.

This Article describes the contours of crypto investment contracts, the blockchain technology, and the markets for blockchain offerings. Part I identifies the structural heterogeneity of blockchain offerings in their varied sources of underlying values, language and corporate forms, technical feasibilities, marketing venues, and voice and exit rights granted to their holders. Unbundling the constitutive elements of blockchain offerings allows a better understanding of the emerging technology for investment contracts and a thorough analysis of its potential securities regulation.

Part II then identifies unique costs and risk factors underlying the blockchain-based investment contract. This Article is the first to identify controlling costs, monitoring costs, and systemic risks stemming from the blockchain territory.

SECURITIES REGULATION: CASES AND MATERIALS (8th ed. 2017). Whether tokens, blockchain units, and cryptocurrencies are securities is also relevant to the legal space in which these web-based exchanges operate. Under § 5 of the Exchange Act, it is "unlawful for any broker, dealer, or exchange . . . to effect any transaction in a security, or to report [it], unless such exchange (1) is registered as [a] national securities exchange," unless an exemption applies. 15 U.S.C. § 78e (2012).

9. Juan Batiz-Benet et al., *The SAFT Project: Toward a Compliant Token Sale Framework* 15–21 (Oct. 2, 2017), https://saftproject.com/static/SAFT-Project-Whitepaper.pdf (proposing a framework to "navigate the federal securities and money-transmitter laws"). *But see Not So Fast—Risks Related to the Use of a "SAFT" for Token Sales*, CARDOZO BLOCKCHAIN PROJECT 1 (Nov. 21, 2017) [hereinafter CARDOZO BLOCKCHAIN PROJECT] (cautioning that the SAFT framework "may create more problems than it solves"). The SAFT is based on the Simple Agreement for Future Equity (SAFE), which has long financed early stage companies. Batiz-Benet et al., *supra* note 9, at 15. In an example of a SAFT transaction, investors would rely on Rule 506(c) of Regulation D of the Securities Act and enter into an agreement with developers to exchange $15 million for tokens through a four-step process. *Id.* at 16.

Part III reviews the theoretical justifications for securities regulation and considers their application to blockchain-investments. The descriptive analysis of the blockchain-based asset is merged with theoretical justifications of securities regulations, explaining why and when crypto-markets fail to protect investors and regulation is warranted. The analysis sheds light on the adequacy of securities regulation of blockchain offerings, while also providing an important case study for analysis of core theoretical questions in securities laws, their purpose, the breadth of their application in different types of markets, and their regulatory exclusivity.

Part IV evaluates types of policies that can be effective in protecting investors from identified sources of risk while facilitating effective functioning of crypto markets and thereby encouraging technological and financial innovation.

The analysis shows that blockchain's new investor interface sometimes replaces the need for securities regulation, providing an automated platform that mitigates the traditional risks of investments and establishes trust based on computation protocols. There are also instances in which the emerging blockchain technology heightens the need for regulating crypto offerings: when the blockchain technology impedes transparency, increases risk, and compromises investors' protection. Understanding the technical and legal differences between various blockchain offerings is key to assessing their potential securities regulation.

The focal point of the discussion assessing the applicability of securities laws to investment contracts is the Supreme Court's opinion in *SEC v. W. J. Howey Co.* (*Howey*),[10] as recently applied by the SEC to the blockchain paradigm in the case of The Decentralized Autonomous Organization (DAO) offering.[11] According to the *Howey* opinion, investors' motivation for profits and their reliance on the efforts of others to accumulate profits is the litmus test of a security.[12] This Article shows that blockchain-based assets call into question the rationality of this doctrine. Reliance on others is an unfit legal test for a decentralized platform, where investors rely on a global community of very many others, none of whom are particularly well-suited to carry the costs of mandatory disclosure. The purchaser motivation test unnecessarily increases regulatory uncertainty looming over the blockchain industry, as purchaser motivation is rarely free of profit aspirations in the blockchain

10. 328 U.S. 293 (1946).
11. *See infra* Section IV.A.2.
12. *See infra* Section IV.A.1.

territory.[13] Additionally, the monitoring costs underlying blockchain-based assets representing consumptive values are often higher, warranting better investor protection, contrary to the *Howey* prescription.

Once the sources of risk are identified, it can be inferred when securities regulation may add value and protect investors. When controlling costs, monitoring costs, and systemic risks, *inter alia*, outweigh the costs of regulation on a blockchain-based asset, securities regulation may be warranted. Drawing on literature from "antifraud only" governance for institutions in the growing 144(a) market,[14] the case is made for analogous public policy allowing sophisticated investors secondary trading with substantial liquidity in blockchain transactions, largely free from securities regulations.[15] Finally, this Article surveys other ways that regulators may address risks of investment in blockchain-based assets, whether supplementing securities laws or as alternative regulatory baskets.

---

13. The costs of uncertainty in the blockchain industry are profound. *See* Peter Van Valkenburgh, *Principles for Clarifying SEC Jurisdiction over Cryptocurrencies and ICOs*, COIN CTR. (May 24, 2018), https://coincenter.org/entry/principles-for-clarifying-sec-jurisdiction-over-cryptocurrencies-and-icos (arguing that the flexibility of the *Howey* test harms innovation and makes the United States "an unfriendly home for earnest technologists whose activities are not fraud and do not pose undue risks to investors," and makes the secondary cryptocurrencies markets "unnecessarily fraught" as there is large uncertainty as to whether all tokens—or only a select few—are securities).

14. *See, e.g.*, 17 C.F.R. § 230.144A (2018); COX ET AL., *supra* note 8, at 379–80 (explaining that Rule 144A "sets forth a non-exclusive safe harbor from the registration requirements of Section 5 of the Securities Act for the resale of restricted securities"); Stephen Choi, *Regulating Investors Not Issuers: A Market-Based Proposal*, 88 CAL. L. REV. 279, 285 (2000) (referring to sophisticated investors as "issuer-level investors" and proposing that "securities of issuers that deal solely with issuer-level investors . . . face no mandatory regulations"); C. Edward Fletcher, III, *Sophisticated Investors Under the Federal Securities Laws*, 1988 DUKE L.J. 1081, 1144 (1988) ("[W]hen only sophisticated investors generally purchase a type of instrument, courts are more likely to consider that instrument not a 'security.'"); William K. Sjostrom, Jr., *The Birth of Rule 144A Equity Offerings*, 56 UCLA L. REV. 409, 417 (2008).

15. The case for such a private market is weighted against expected political hurdles, including the motivation of securities regulators to police the financial powers emerging on the blockchain, implicitly imposing such norms as accountability and transparency on the libertarian sphere of the blockchain, largely detached from the monetary governance of the state. *See generally* Roberta Romano, *The Need for Competition in International Securities Regulation*, 2 Theoretical Inq. L. 387, 393–94 (2001). *Cf.* Donald C. Langevoort, *The SEC, Retail Investors, and the Institutionalization of the Securities Markets*, 95 VA. L. REV. 1025, 1027 (2009) (questioning whether the SEC should be tasked with regulating the increasingly global and technical financial marketplace).

I. THE PROPERTIES OF BLOCKCHAIN-BASED ASSETS

This Section provides a factual background for analyzing blockchain-based assets as securities. The technology of the blockchain is introduced, shedding light on the heterogeneous technical applications of blockchain-based assets, the varied entry costs for their offerors, and the open code vulnerabilities, including consensus protocols and blockchain "forks." The different sources of values attached to blockchain-based assets are elaborated, introducing the concepts of "utility tokens" versus "investment tokens," and the substantial value attributed to the size of their user networks. Marketing venues of blockchain-based assets are reviewed. Finally, this Section surveys the language used by blockchain-based investment contracts, the diversity of their corporate forms, the language of the blockchain investment contract, and the exit and voice rights conferred upon blockchain investors.

A. The Technology

The blockchain-based assets discussed in this Article are technologically embedded in a ledger in which all transactions are maintained by a network of nodes (computers) that coordinate to maintain and extend its content. The generic term "blockchain-based assets" is used to refer to virtual assets where issuance and ownership are defined by blockchains—or "cryptocurrency coins" and "tokens," in the blockchain industry's terminology.

The ledger consists of a sequence of records, each representing a transaction with precisely defined format and semantics.[16] These transactions are in virtual assets associated with the blockchain and may represent the issuance of new units of such assets, transfer of ownership in such units, or more generally a specification for how certain units of the assets will be automatically allocated under specified conditions of a so-called "smart contract."[17]

A ledger implemented by a blockchain can be decentralized or centralized[18] and "permissioned" or "permissionless"—i.e., requires or does

16. The ledger compiles documents together in a tree structure (a chain) and timestamps each document/transaction as it is appended. *See* ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION XX–XXI (2016).

17. A "smart contract" is defined as "an agreement whose execution is automated." Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 309 (2017).

18. An example of a decentralized system is Bitcoin, which "has no central points of control, and uses a novel peer-to-peer network protocol to agree on a distributed

not require permission to read and add transaction records.[19] In a centralized ledger, one party or organization, runs the software on the blockchain and exclusively controls the database embedded in its ledger.[20] In a decentralized ledger, the computation and maintenance are run on network nodes that are dispersed and no single party controls the network.[21]

Another property of blockchain is the permission to read and to write on the ledger: defining the agents allowed to issue new transactions and the agents allowed to read the content of transactions already recorded in the ledger. In a permissionless ledger, any party can post new valid transactions for inclusion in future blocks using the consensus protocol, and any party is allowed to read all past transactions.[22] The validity of a transaction depends on its content—e.g., the transaction does not create funds out of thin air in violation of the protocol, and transfer of ownership in the blockchain-based asset is authorized by a digital signature of the previous owner—but does not depend on the identity of the party that transmits the transaction.[23] Conversely, in a permissioned ledger, addition and/or reading of transaction records can be done only by specific designated parties.[24] In general, permission has to with content of the blockchain,

---

ledger of transactions." CHELSEA BARABAS ET AL., MIT MEDIA LAB, *Defending internet Freedom Through Decentralization: Back to the Future?* 1 (2017). Most of today's prominent blockchains are decentralized, e.g., Bitcoin, Ethereum, and Litecoin.

19. Ramesh Gopinath, *Checking the Ledger: Permissioned vs. Permissionless Blockchains*, IBM THINK BLOG (July 28, 2016), https://www.ibm.com/blogs/think/2016/07/checking-the-ledger-permissioned-vs-permissionless-blockchains (arguing that permissioned blockchains are preferable to permissionless blockchains because they promote economic activity and efficiency, reduce potential for disputes, and are more easily regulated).

20. Taulant Ramabaja, *On Centralized vs Decentralized Ledgers*, BITSAPPHIRE (Feb. 12, 2015), https://bitsapphire.com/on-centralized-vs-decentralized-ledgers (noting the general belief that the Internet, Bitcoin, and other evolving technologies could cripple the system of central powers controlling networks).

21. *See* Heidi Hecht, *Decentralization vs Centralization*, CRYPTO BRIEFING, https://cryptobriefing.com/decentralization-vs-centralization (last updated Aug. 25, 2018) (noting that with decentralization "there's no centralized third party controlling [] platforms").

22. *See Permissioned vs Permissionless Ledgers*, 1KOSMOS BLOCKID (June 5, 2018), https://onekosmos.com/blog/permissioned-blockchain-vs-permissionless-ledgers ("Permissionless blockchains . . . [are] open for anyone to participate [in] . . . and have open-source code that their community maintains.").

23. *See infra* note 24 and accompanying text.

24. Permissioned ledgers are of interest mainly in business-to-business and enterprise applications. *Cf.* Sloane Brakeville & Bhargav Perepa, *Blockchain Basics: Introduction to Distributed Ledgers*, IMB: DEVELOPERWORKS (Mar. 18, 2018), https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs (stating that "industrial-grade blockchain technologies" should be

and centralization has to do with its platform, or technical infrastructure. To illustrate, it may be useful to a consider an analogy to a radio program, centralized through the radio station's broadcast. The sportscast would be considered permissioned, while the request show inviting listeners to call-in would be permissionless.

Ownership of blockchain-based assets is authoritatively defined by the transactions recorded in the current version of the ledger.[25] The ledger keeps evolving as new transactions are appended.[26] Parties that wish to view or add to the ledger run a designated computational protocol, embedded in computer software, which communicates with other such parties to establish a consistent view of the blockchain.[27] The process of obtaining a consistent ledger in a decentralized, permissionless blockchain is based on a consensus protocol.[28] Numerous nodes communicate by a designated "consensus protocol" to vote on which updates to embed into the ledger, aiming to make the ledger resilient to opportunistic intervention, manipulation, and censorship. The nodes that participate in this consensus protocol are termed "miners."[29] The decision on the contents of the new block cannot be made by naïve voting among miners due to the threat of "Sybil" attacks where a single party masquerades as numerous nodes.[30]

---

permissioned). Blockchain platforms designed for permission ledgers include Hyperledger Fabric and R3 Corda. *See* MARTIN VALENTA & PHILIPP SANDNER, FRANKFURT SCH. BLOCKCHAIN CTR., *Comparison of Ethereum, Hyperledger Fabric and Corda* 2 (2017), http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf (identifying Hyperledger Fabric and R3 Corda as "[p]ermissioned, private" ledgers).

25. Amy Castor, *A (Short) Guide to Blockchain Consensus Protocols*, COINDESK, https://www.coindesk.com/short-guide-blockchain-consensus-protocols (last updated May 17, 2017, 5:11 PM) (explaining the significance of a "consensus algorithm").

26. For example, with Bitcoin, "a new block is appended to the blockchain every 10 minutes, through mining." *Blockchain*, INVESTOPEDIA, https://www.investopedia.com/terms/b/blockchain.asp (last visited Oct. 17, 2018).

27. *See* Castor, *supra* note 25 (explaining various methods of proving the veracity of the ledger).

28. *See Introduction*, HYPERLEDGER FABRIC, https://hyperledger-fabric.readthedocs.io/en/release-1.2/blockchain.html (last visited Oct. 17, 2018) (explaining how consensus operates in a decentralized blockchain ledger for Hyperledger Fabric v1.2).

29. *See* Noelle Acheson, *How Bitcoin Mining Works*, COINDESK, https://www.coindesk.com/information/how-bitcoin-mining-works (last updated Jan. 29, 2018) (explaining "nodes" and which types constitute "miners").

30. "A Sybil attack . . . occurs when a hacker presents many different identities and manipulates the blockchain to the hacker's benefit." Jane Susskind, Comment, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, 54 SAN DIEGO L. REV. 785, 814 (2017) (citing Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 386–90 (2016)).

Thus, consensus protocols use weighted voting, where the weight of a miner's vote, relative to other miners, depends on some measure of resource investment. Details vary, but currently, most blockchains rely on "proof-of-work," where votes are effectively weighed according to the amount of computational effort spent solving mathematical puzzles.[31] Thus, in a decentralized blockchain, miners are not equal in their control, but are given equal terms that can, at the miners' discretion, acquire control by ad hoc resource consumption and/or capital investment. In Bitcoin (BTC), for example, the consensus protocol is based on a proof-of-work requirement that is essentially a collateral of computational power.[32] Bitcoin's consensus protocol chooses a particular node in the network and makes it the "king" of the new block, granting it the exclusive power to assign and allocate ownership in the new block, subject to compliance with the node's requirements.[33] The winning node is not chosen at random.[34] Bitcoin applies a proof-of-work mechanism that is based on solving a mathematical puzzle.[35] For every new block, a new puzzle is created, and the first node to solve that puzzle will get the privilege of allocating the property rights within the new block.[36] The number of blocks one previously runs or owns, and the number of nodes one possesses, are therefore irrelevant regarding the ability to generate new nodes. The power to assign and allocate property rights on Bitcoin's blockchain is thus a function of the computational power one has.[37]

---

31. Proof-of-work essentially measures the computer hardware capital and energy (for running and cooling the computers) that were dedicated to mining. *See* Castor, *supra* note 25 (explaining the proof-of-work process). Emerging alternative approaches include, *inter alia*, proof-of-space (measuring capital in the form of computer storage resources that is dedicated to mining) and proof-of-stake (consisting of capital in the form of blockchain-based assets that is locked up for the duration of mining).

32. *See Bitcoin Developer Guide*, BITCOIN, https://bitcoin.org/en/developer-guide#proof-of-work (last visited Oct. 17, 2018) (explaining how a greater degree of computational work is essentially imposed on "untrustworthy" actors as a way to regulate the Bitcoin market).

33. *Cf.* Acheson, *supra* note 29 (explaining nodes, miners, hash functions, and how Bitcoin generally works).

34. *See id.* (explaining the process through which miners compete to solve the winning number in the hash function in exchange for 12.5 bitcoins, which was roughly worth $200,000).

35. *Id.*

36. *Id.*

37. *See* Andrew Tar, *Proof-of-Work, Explained*, COINTELEGRAPH (Jan. 17, 2018), https://cointelegraph.com/explained/proof-of-work-explained ("What matters is to have large computational power to solve puzzles and form new blocks.").

Computational power entails significant costs, including computer equipment subject to depreciation,[38] electricity costs to run the computers, and cooling costs of the heat generated by the computers.[39] Both electricity costs and cooling costs are consumable goods. These costs function as quasi-collateral. As an incentive to parties to invest such computational effort and apply it to the blockchain's network, some blockchains assign a mining fee.[40] In Bitcoin, the mining fee is predetermined by a formula according to a fee schedule and transaction fees are collected from holders of allocated units in the designated block.[41] In theory, any node can participate in the bidding process on computational power.[42] In practice, however, the significant costs of computational effort required leave a limited set of agents in the field, creating a quasi-oligopoly of miners who employ large "mining farms" with numerous servers dedicated to the process of bidding for new blocks, often in rural and remote locations where electricity costs are lower and cooling costs are naturally available due to weather conditions.[43]

---

38. Computer hardware typically needs to be replaced every two years to remain competitive. Mark Kyrnin, *Upgrade or Replace a Desktop PC?*, LIFEWIRE (Nov. 1, 2017), https://www.lifewire.com/upgrade-or-replace-desktop-pc-832712 (noting that "[t]he average desktop PC has a functional lifespan of roughly three to eight years").

39. *See* Aaron Hankin, *Here's How Much It Costs to Mine a Single Bitcoin in Your Country*, MARKETWATCH (May 11, 2018, 9:18 AM), https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06 (noting a study that indicated costs ranged from $531 to $26,170 per bitcoin mined and that energy consumed worldwide mining bitcoins is equivalent to the Czech Republic's annual energy usage); Jordan Tuwiner, *Is Bitcoin Mining Profitable or Worth It in 2018?*, BUY BITCOIN WORLDWIDE, https://www.buybitcoinworldwide.com/mining/profitability (last updated June 30, 2018) (noting that "[o]nly those with specialised [sic], high-powered machinery . . . are able to profitably extract bitcoins nowadays" and that the difficulty of mining bitcoin has grown exponentially in recent years).

40. *What is the Blockchain Fee?*, WIREX, https://help.wirexapp.com/hc/en-us/articles/212638865-What-is-the-blockchain-fee (last visited Oct. 17, 2018) (noting the mining fee "is collected to reward miners for maintaining the Bitcoin network").

41. *See* Gautham, *Bitcoin Miner Fees and Micropayment Channels*, NEWSBTC (May 22, 2016, 9:30 PM), https://www.newsbtc.com/2016/05/22/bitcoin-miner-fee-and-micropayment-channels (explaining the "fee predictor" and small block size).

42. *See* Euny Hong, *How Does Bitcoin Mining Work?*, INVESTOPEDIA, https://www.investopedia.com/tech/how-does-bitcoin-mining-work (last updated July 2, 2018, 8:00 AM) (noting only computing power is needed, not math or computational skills).

43. *See* Morgen E. Peck, *Why the Biggest Bitcoin Mines are in China*, IEEE SPECTRUM (Oct. 4, 2017, 7:00 PM), https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china (describing a large facility in Mongolia composed of 21,000 computers, and climate and energy costs as factors in determining the location of a mining farm); Jordan Tuwiner, *Bitcoin Mining Pools*, BUY BITCOIN WORLDWIDE, https://www.buybitcoinworldwide.com/mining/pools (last updated June 30, 2018)

Most blockchains are implemented by open source software, distributed under licenses that allow copying and modification.[44] Modifications to the software may continue obeying the same consensus rules, and thus agree with the original software about what is the authoritative version of the ledger and what asset ownership it reflects.[45] Conversely, modifications may change these rules, thereby inducing a "fork" of the chain, where parties using the old software see one version of the transaction history and parties using the new software see a different version.[46] For example, if specific transactions in the ledger are deemed unpalatable by some parties, then it is technically feasible and legally permissible to fork the blockchain into a new one, which is similar to the original except that those specific transactions are nullified—and any user of the blockchain who chooses to upgrade its software would accordingly view a different transaction history on the ledger.[47] A fork may also be created to upgrade the blockchain for better performance or functionality,[48] or to launch a competing blockchain and capture market share.[49]

(describing various mining pools and stating they "are groups of cooperating miners who agree to share block rewards in proportion to their contributed mining hash power").

44. *See* Demian Stauber, *Spotlight on Copyright Issues of Blockchain Technology*, FRORIEP (Sept. 21, 2017, 2:45 PM), https://blog.froriep.com/en/spotlight-on-copyright-issues-of-blockchain-technology (noting that "[m]ost public known blockchain projects are open source," which means their software allows for free redistribution and modification permissions).

45. *See* Amy Castor, *A Short Guide to Bitcoin Forks*, COINDESK, https://www.coindesk.com/short-guide-bitcoin-forks-explained (last updated May 16, 2017, 9:05 PM) (explaining "soft forks" and how new transactions may still appear valid to non-upgraded nodes).

46. For a history of consensus forks on Bitcoin, see *A Complete History of Bitcoin's Consensus Forks*, BITMEX (Dec. 28, 2017), https://blog.bitmex.com/bitcoins-consensus-forks.

47. This is the case, for example, in the Ethereum/Ethereum Classic fork, intended to nullify specific fraudulent transactions in the DAO. *See infra* Section III.E (DAO fork).

48. For example, consider the fork between Bitcoin and Bitcoin-cash executed in August 2016. The upgraded version of bitcoin incorporated SegWit, a protocol enhancement designed to reduce the size of transaction records, was named Bitcoin, while the original version became known as "bitcoin cash." *See* Jacqui Frank et al., *We Just Got a Super Smart and Simple Explanation of What a Bitcoin Fork Actually Is*, BUS. INSIDER (Nov. 1, 2017, 4:02 PM), https://www.businessinsider.com/bitcoin-fork-explained-gold-segwit-segwit2x-cash-the-bit-3-2017-10; *Making Bitcoin Work Better*, THE ECONOMIST (July 29, 2017), https://www.economist.com/finance-and-economics/2017/07/29/making-bitcoin-work-better. Interestingly, the branding of different forks of the blockchain is decided ad-hoc by market forces and eco-system politics.

49. *See* Jake Smith, *The Bitcoin Cash Hard Fork Will Show Us Which Coin Is Best*, FORTUNE (Aug. 11, 2017), http://fortune.com/2017/08/11/bitcoin-cash-hard-fork-price-date-why (noting the split allowed for competition and assuaged fears by some of centralization).

Some blockchains support the ad hoc creation of new asset types. Most notably, Ethereum supports the creation of "ERC-20 tokens," which are new asset types that can be transacted on the Ethereum blockchain—in addition to, and separately from, the native "ether" blockchain-based asset (ETH).[50] Anyone can create such a token and set the token supply and distribution rules at their discretion.[51] The technical implementation of such tokens—e.g., the consensus protocol and supporting software—is mostly provided by the underlying, pre-existing Ethereum blockchain platform.[52] This creates a very low barrier to entry for creation of new blockchain-based assets that are simple tokens without an independent blockchain.[53]

Blockchain technology has thus established:

(1) The means of creating virtual assets—"tokens," or "cryptocurrencies"—and assigning such assets an underlying value implemented via code, contract, collateral, etc.[54]

(2) A quantitative methodology for allocating ownership in these virtual assets and representing it publicly on a ledger, analogous to a registry of deeds.[55]

(3) A platform for trade in these virtual assets, conveniently and efficiently, in exchange for Bitcoins, Ether (ETH), or other cryptocurrencies, all easily exchangeable for U.S. dollars (USD) and other major international currencies on the web.[56]

---

50. Nathan Reiff, *What is ERC-20 and What Does it Mean for Ethereum?*, INVESTOPEDIA (June 20, 2017, 9:36 AM), https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum (explaining ERC-20 and Ethereum, and distinguishing them from ether).

51. *See id.* (noting ERC-20's impact on developers and that new tokens released by developers "have by-and-large observed the ERC-20 rules").

52. *See id.* (listing six different functions that ERC-20 defines).

53. *See* James Cheo, *Why Blockchain is Real and Bitcoin is a Mirage*, FORBES (Dec. 10, 2017, 11:27 PM), https://www.forbes.com/sites/insideasia/2017/12/10/why-blockchain-is-real-and-bitcoin-is-a-mirage (noting the aggregate infiniteness of cryptocurrencies and the low barrier to entry regarding creation of new cryptocurrencies).

54. *See id.* (commenting that Bitcoin is a multi-billion dollar virtual asset, and explaining blockchain and its potentially wide-ranging applications).

55. *See id.* ("A blockchain is essentially a distributed database of records or public ledger of all transactions that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus—a majority of the participants in the system.").

56. *See, e.g.*, *About*, KRAKEN BITCOIN EXCHANGE, https://www.kraken.com/en-us/about (last visited Oct. 17, 2018) (explaining how Kraken allows users to exchange Bitcoin for European Union, Canadian, American, British, or Japanese currencies). Whether blockchain-based assets are securities is also relevant to the legal space in which these web-based exchanges operate. Under § 5 of the Exchange Act, it is

When the supply of assets created by this technology meets demand, a market is established.

B. The Market

Notably, many blockchain-based assets are not offered to the public in the primary market.[57] For example, Bitcoin was released as an open source software, submitting to a decentralized mining process shortly after a white paper was published describing its concept.[58] The period between the launch of the blockchain-based asset and the public release of its code is often referred to as a pre-mining period, giving entrepreneurs a period of privileged mining with lower costs and no competition.[59]

Tokens or cryptocurrencies may be offered to the public, typically, in a process entitled an initial coin offering (ICO), alluding to initial public offering (IPO) of securities in the traditional market place.[60] ICOs raise capital through allocation of blockchain units and are often accompanied by a public relations campaign, aimed to raise a specific target of funding

---

unlawful to engage in any transaction in a security not registered on a national exchange, unless an exemption applies. 15 U.S.C. § 78e (2012). An "exchange" is defined as "any organization, association, or group of persons [which] . . . provides a market place or facilities for bringing together purchasers and sellers of securities." § 78c(a)(1). Exchange Act Rule 3b-16(a) provides a functional test to assess whether a trading system meets the definition of exchange under § 3(a)(1): "[a]n organization, association, or group of persons shall be considered" an exchange if it "(1) [b]rings together the orders for securities of multiple buyers and sellers; and (2) [u]ses established, non-discretionary methods . . . under which such orders interact with each other . . . ." 17 C.F.R. § 240.3b-16(a) (2017). This rule excludes systems that merely "[r]oute[] orders to" other execution facilities. *Id.* § 240.3b-16(b)(1). One such exemption is the Alternative Trading Systems (ATSs), defined by Rule 300(a) of Regulation ATS, which exempts platforms that do not "[s]et rules governing the conduct of subscribers other than the conduct of such subscribers' trading on such [ATSs]" or "[d]isciplines subscribers other than by exclusion from trading." *Id.* § 242.300(a)(2).

57. *See, e.g.*, Michael Scott, *Private Capital Market Ecosystems Meet the Blockchain*, BITCOIN MAG. (June 6, 2017, 1:27 PM), https://bitcoinmagazine.com/articles/private-capital-market-ecosystems-meet-blockchain (describing "an agreement to build an alternative investment marketplace for closed-end funds utilizing [blockchain]").

58. *See infra* Section IV.D.1 (providing a detailed analysis of Bitcoin).

59. For a discussion of pre-mining, see Antonio Madeira, *What is a Premine?*, CRYPTOCOMPARE (May 20, 2018), https://www.cryptocompare.com/coins/guides/what-is-a-premine.

60. *The Meaning in the Madness of Initial Coin Offerings*, THE ECONOMIST (Nov. 9, 2017), https://www.economist.com/leaders/2017/11/09/the-meaning-in-the-madness-of-initial-coin-offerings (describing ICOs as "a form of crowdfunding" where coins are exchanged for payment).

and bounded in a particular time frame for the offering.[61] Many ICOs are accompanied by a white paper or a "plan," describing the merits of the proposed investment offer, although officially the contractual language is embedded in the consensus algorithm (or the smart contract), and the white paper subordinates to the code's terms.[62]

One key distinction between crypto markets and traditional capital markets is the original number of units offered for sale. In traditional capital markets, the number of units offered is explicitly stated in the offering memoranda. For example, an IPO is an offering of a fixed number of shares to be sold.[63] Trade in secondary markets is therefore capped to the fixed amount of securities available. In crypto markets, on the other hand, the number of units is constantly growing through an on-going mining process.[64] The original offer typically defines a "genesis block" that sets the mining challenge and identifies the process for recreating future blocks that are added to the blockchain.[65] Some blockchains set a maximum cap ("limited money supply" in the blockchain rhetoric), while others have an endless continuum available for mining.[66] Notably, in both

---

61. *Initial Coin Offering (ICO)*, INVESTOPEDIA, https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp (last visited Oct. 17, 2018) [hereinafter ICO] (outlining the ICO process).

62. *Id.* *See* Cohney et al., *infra* note 96, at 6 (documenting a consistent "gap between what ICOs promise and what their code delivers").

63. Royce de Rohan Barondes, *Correcting the Empirical Foundations of IPO-pricing Regulation*, 33 FLA. ST. U. L. REV. 437, 441–42 (2005) (providing background information on the IPO process and describing the way in which IPOs are sold); *see also* Sham Gad, *How an IPO is Valued*, INVESTOPEDIA, https://www.investopedia.com/articles/financial-theory/11/how-an-ipo-is-valued.asp (last updated Apr. 3, 2018, 10:23 AM) (noting the price of a share is dependent upon its demand).

64. *See Mining*, TECHOPEDIA, https://www.techopedia.com/definition/32530/mining-blockchain (last visited Oct. 17, 2018) (defining mining as "the process of adding transactions to the large distributed public ledger of existing transactions, known as the blockchain").

65. A genesis block is the first block in the chain. *See Genesis Block*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Genesis_block (last visited Oct. 17, 2018) (noting that the genesis block is special in that it does not reference a previous block and contains "exactly all of the variables necessary to recreate the block").

66. For a discussion of Bitcoin's limited supply, see *Controlled Supply*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Controlled_supply (last visited Oct. 17, 2018), which provides that there will only be a finite number of bitcoins in existence because the number of bitcoins created per block is set to decrease. Unlike Bitcoin, Ethereum does not have a specific currency supply limit. *See Ethereum Not Having a Supply Cap Is Not Such a Big Deal*, FINTECHIST, http://www.fintechist.com/ethereum-not-supply-cap-not-big-deal (last visited Oct. 17, 2018). For a detailed comparison of Bitcoin and Ethereum, see *Bitcoin vs Ethereum: Where to Invest in the Next 10 Years?*, CRYPTOCURRY, http://cryptocurry.com/features/bitcoin-vs-ethereum-invest-next-10-years (last visited

cases, the original offer does not encompass the entire holdings available in blockchain-based assets, and these holdings are expected to continuously grow with the mining process over time.

In the secondary market, trade in tokens and cryptocurrencies is often conducted on web platforms that allow online market spaces for forex, stocks, commodities, derivatives and indices. Examples for such web-based exchange platforms include Gemini,[67] Coinbase,[68] CoinMarketCap,[69] and AvaTrade.[70] Yet the crypto secondary markets are fundamentally different from traditional capital markets. The traditional market-based antidotes—signaling, underwriter reputation, and accountant or credit-rating certification—simply do not apply as there are no underwriters, analysts, credit rating agencies, or accountants in the crypto context. The sale is often automated so that a smart contract is programmed to allocate tokens to third parties immediately after payment has been received.[71] There are no intermediaries,[72] and no systematic analyst coverage, other than emerging crypto analyst firm Messari[73] and occasional reviews by bloggers of different backgrounds and views.

C. The Transaction

This section introduces the transactional structure of blockchain-based assets, drawing attention to the nature of the complexity embedded in these innovative constructs. It examines the varied sources of value embedded in blockchain-based assets, the language used for

---

Oct. 17, 2018) [hereinafter *Bitcoin vs Ethereum*] (describing the key differences between Bitcoin and Ethereum, including the time to process blocks, the depth of their monetary supply, the pricing of transactions, and the structure of their internal codes).

67. *See* GEMINI, https://gemini.com (last visited Oct. 17, 2018).

68. *See* COINBASE, https://www.coinbase.com (last visited Oct. 17, 2018).

69. *See* COINMARKETCAP, https://coinmarketcap.com (last visited Oct. 17, 2018).

70. *See* AVATRADE, http://www.avatrade.com (last visited Oct. 17, 2018).

71. *See* Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain* 8 (Nat'l Bureau of Econ. Research, Working Paper No. 22952, 2018), http://www.nber.org/papers/w22952.pdf (explaining that smart contracts are specific operations that "can be automated in response to future events," such as receiving payments from third parties).

72. *Id.* at 6, 8–9 (clarifying that transactions in the crypto secondary markets utilize blockchain technology instead of intermediaries).

73. *About*, MESSARI, https://messari.io/about (last visited Oct. 17, 2018) (stating that Messari's mission is to "help[] researchers, investors, and regulators" make sense of cryptocurrencies through an open data library and curation tools).

blockchain-based contracts, the heterogeneous corporate forms used by their developers, and the exit and voice rights given to their investors.

1. Value

Blockchain transactions vary in their underlying sources of value. Sometimes, the value of blockchain-based assets is intrinsic to the blockchain itself—such value can be embedded in the blockchain's technological merit, in its software, and/or in the size of its user network.[74] Other blockchain-based assets represent values off their chain, such as consumptive goods or services, often in entrepreneurial stages.[75]

Consider, for example, Bitcoin's sources of value. Some of Bitcoin's value is derived out of its technological merit as a method for safe, efficient, and fast transfer of financial value to anyone all over the world.[76] The expediency of value transfer in cryptocurrencies is practically useful to merchants in globally spread supply chains, compared with the traditional bank transfer of currencies abroad which may take up to a week.[77] On top of this practical value, the value of Bitcoins is also derived from the size of its network of Bitcoin users and its expected market value in the secondary market, due to its growing reputation and expanded user network.[78]

---

74. Bitcoin is one example that may be considered to understand how the value of blockchain-based assets is determined. *See Bitcoin*, INVESTOPEDIA, https://www.investopedia.com/terms/b/bitcoin.asp (last visited Oct. 17, 2018) (stating that the price of Bitcoin depends on the size of its mining network).

75. *See infra* notes 290–310 and accompanying text (discussing Tezos and Filecoin).

76. CHRIS BURNISKE & JACK TARTAR, CRYPTOASSETS: THE INNOVATIVE INVESTOR'S GUIDE TO BITCOIN AND BEYOND 176 (2018). Cryptocurrencies offer an online system for immediate transfer of value any date or time, whereas international financial transactions can take days to process and are often subject to regulatory approval and to the business hours of the financial intermediaries involved. *Id.*

77. *Id.*

78. Regarding Bitcoin, funds are not raised with the expectation that the promoters will build their system and investors can earn a return on the instrument. Rather, funds reflect the size of the network and the expectation to collect accumulated returns based on the extension of such network. The core algorithm remains unchanged. Cryptocurrencies and tokens often appreciate their value with the extension of their respective user networks. An evaluation of bitcoin based on its network of users has been suggested by Tom Lee. *See* Sara Silverstein, *Analyst Says 94% of Bitcoin's Price Movement over the Past 4 Years can be Explained by One Equation*, BUS. INSIDER (Nov. 10, 2017, 9:51 AM), https://www.businessinsider.com/bitcoin-price-movement-explained-by-one-equation-fundstrat-tom-lee-metcalf-law-network-effect-2017-10. Spencer Wheatley et al. show that the key measure of value for cryptocurrencies is the network of people who use them by documenting a generalized Metcalfe's law describing the growth of the population of active bitcoin users, showing

The network value of cryptocurrencies is sometimes called the "Tinkerbell Effect," alluding to the fictional world of Peter Pan.[79] Tinkerbell exists only as long as one believes in her, and the value of blockchain-based assets exists not because some central bank will serve as a liquidity backstop, but because the size of their network of users sustains a constant flow of demand in the secondary market, which indirectly gives the blockchain-base assets market value.[80] In that sense, blockchain-based assets are similar to commodities, the value of which is an aggregate sum of its practical value for the end user and its network value, entrenched in the consumer perception of the commodity within the social environment at which it is sold.[81]

Other blockchain units are contractually designed to represent value in another product or service extrinsic to the blockchain.[82] The plan or white paper accompanying the offering often attaches underlying initiatives to the blockchain so that allocation of blockchain units represent respective ownership stakes in an asset, project, or business initiative in the real economy.[83] Often, such a project has not been undertaken or even initiated at the time the ICO is carried out, and the ICO is an entrepreneurial proposal that is yet to be materialized and performed by the offeror or offerors. Examples include

---

that the generalized Metcalfe's law provides a support level, and that the ratio of market capitalization to "the Metcalfe value" gives a relative valuation ratio. Spencer Wheatley et al., *Are Bitcoin Bubbles Predictable? Combining a Generalized Metcalfe's Law and the LPPLS Model* 2, 13–14 (Swiss Fin. Inst., Paper No. 18-22, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3141050; *see also How Network Theory Predicts the Value of Bitcoin*, MIT TECH. REV. (Mar. 29, 2018), https://www.technologyreview.com/s/610614/how-network-theory-predicts-the-value-of-bitcoin.

79. For a discussion of the analogy between Bitcoin appreciation and the Tinkerbell Effect, see NARAYANAN ET AL., *supra* note 16, at 169.

80. *Id.*

81. For example, the value of gold is expected to appreciate with growth of its social prestige and its public image as a luxury metal. *See supra* note 78 (discussing Bitcoin valuation using Metcalfe's law). A recent district court decision found in favor for the Commodity Futures Trading Commission (CFTC) and held that Bitcoin is a commodity under the Commodities Exchange Act because of the way cryptocurrencies store value and influence the economic behavior of users, as well as serving as a type of monetary exchange. *See* CFTC v. McDonnell, 287 F. Supp. 3d 213, 224–27 (E.D.N.Y. 2018).

82. *See* Bernard Marr, *What Is The Difference Between Bitcoin and Ethereum?*, FORBES (Feb. 5, 2018, 12:28 AM), https://www.forbes.com/sites/bernardmarr/2018/02/05/what-is-the-difference-between-bitcoin-and-ethereum (explaining that Ethereum is a blockchain-based asset that represents value in Ether, a type of crypto token).

83. For an example of a white paper that accompanies an offering, see *infra* note 304, which contains Filecoin's white paper.

entrepreneurial efforts and endeavors in a particular underlying market, products, or services offered in such an extrinsic underlying market, commodities, indices, and any other form of value.[84] Blockchain-based assets that offer investors the opportunity to use or to consume a valuable service are usually referred to as "utility tokens" and are somewhat analogous to derivative contracts: one layer representing the underlying value and the other representing the unit of blockchain-based asset serving as its platform.[85] Notably, "utility tokens" can represent functional underlying value, such as a commodity or a stake in revenues of an operating business, or other sources of value in the real economy.[86]

However, from a contractual perspective, ICO documents often disclaim any obligation to actually deliver their initiatives or perform specific obligations towards the accomplishment of the proposal.[87] Purchasers of tokens, or other blockchain units under an ICO, are thus exposed to a very high counterparty risk, essentially trusting the offeror to perform their obligations in the real economy; to expand the network so as to raise the tokens' value in the secondary market; and to technically maintain the network so as to secure it against cyber-attacks, hyper-dilution, and bugs in its code.[88] These utility tokens are

---

84. For an illustration of the breadth of potential underlying values for blockchain-based assets, see BANANACOIN, https://bananacoin.io (last visited Oct. 17, 2018) (demonstrating that the Bananacoin is pegged to the export price of one kilogram of bananas). *See* Lionel Laurent, *I've Seen the Blockchain's Future. It's Banana-Shaped*, BLOOMBERG (Jan. 26, 2018, 2:00 AM), https://www.bloomberg.com/gadfly/articles/2018-01-26/i-ve-seen-the-blockchain-s-future-it-s-banana-shaped (exploring how crypto-assets can now be tied to "real-world value rather than mere abstraction").

85. *See* Jonathan Rohr & Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, HASTINGS L.J. (forthcoming 2018) (manuscript at 11, 41, 44–45), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104 (emphasizing the "dual nature" of utility tokens by explaining how they have both a practical use and a derived value that can be used as an investment opportunity).

86. For an overview of utility tokens, see CARDOZO BLOCKCHAIN PROJECT, *supra* note 9, at 2.

87. *See* Zetzsche et al., *infra* note 158, at 12, 17 (identifying the contractual risks that ICO documents, such as white papers, pose).

88. *See* Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11 (addressing several concerns about the cryptocurrency markets and warning investors about the various risks associated with ICOs); *see also* Nathan Reiff, *ICOs Present Unique Legal Risk to Buyers and Sellers*, INVESTOPEDIA (Feb. 27, 2018, 5:00 AM), https://www.investopedia .com/news/icos-present-unique-legal-risk-buyers-and-sellers (describing some of the risks created by ICOs—such as investors "[struggling] with [offerors] that don't follow through on their promises, and the potential for hacks and fraud").

a method of raising initial "seed" funding for an entrepreneurial project, at a point in time when the potential of the project is uncertain, and the project may be abandoned by its entrepreneurs, diluted by other investors, or experience any other material change to its business plan, personnel, or underlying property. Typically, no particular commitment is made by the offerors to dedicate their time and efforts to the planned entrepreneurial project. According to a recent study, "utility tokens represent the majority of tokens issued to date."[89] Another recent study finds that less than 10 percent of the tokens acquired by investors "can be put to use" while the rest are "merely available for trading, indicating purely speculative instruments."[90]

2. Language and corporate forms

The legal terms of the blockchain transactions are rarely accessible to the layman investor. The legally binding terms of the blockchain-based asset are embedded in its code (i.e., the computer software defining its operation).[91] Typically, but not necessarily, this code is open source, and purchasers of tokens may view it prior to the transaction.[92] However, understanding the code requires significant technical expertise and effort. The code is often written in a programming language unique to the blockchain, requiring much effort of experts literate in several programming languages.[93] In addition, offerors of the tokens usually produce a white paper or an unofficial offering memorandum to accompany the offer as part of its marketing efforts.[94] Some other marketing initiatives accompany blockchain offerings, including celebrity endorsements, banner advertisements and other media and press releases, all of which are

89. CARDOZO BLOCKCHAIN PROJECT, *supra* note 9, at 2.

90. Zetzsche et al., *infra* note 158, at 18.

91. *See* Reggie O'Shields, *Smart Contracts: Legal Agreements for the Blockchain*, 21 N.C. BANKING INST. 177, 181 (2017) (noting that the "actual agreement" for a blockchain-based asset "is embodied in computer code").

92. *See* Tanaya Macheel, *R3 Makes Code for Financial Agreements Platform Open Source*, AM. BANKER (Nov. 30, 2016, 9:21 AM), https://www.americanbanker.com/news/r3-makes-code-for-financial-agreements-platform-open-source (discussing one example of a blockchain platform making its code open source).

93. *See Blockchain Coding: The Many Different Languages You Need!*, BLOCKGEEKS, https://blockgeeks.com/guides/blockchain-coding (last visited Oct. 17, 2018) (outlining how to code on a blockchain).

94. *See supra* notes 61–62 and accompanying text.

directed at the general audience and provided in English.[95] Purchasers of blockchain-based assets are generally left to make their decision based on the more accessible and comprehensible marketing materials disseminated by the offerors. Often, these accompanying marketing materials are not including solid contractual obligations of the offerors but rather display their intent to proceed in entrepreneurial efforts as described in the white paper "in future tenses."[96] Indeed, a recent empirical survey of ICOs finds that there is constant gap between contract and code, with significant differences documented between the blockchain's code and its accompanying white paper, suggesting that code often falls short of contract in ICOs.[97]

Offers of blockchain units are initiated by groups of developers using various corporate forms, including for-profits, non-profits, and unincorporated organizations.[98] Some developers use non-profits to signal their societal commitment, characterizing the exchange of the tokens as a donation for tax purposes.[99] It is also not uncommon to see developers offering blockchain units without incorporating at all, using the blockchain itself as an alternative technological liability shield.[100]

3. Exit and voice

While almost all blockchain units offer their holders a right to exit and sell their holdings in the secondary markets, different blockchains vary in the voice given to their holders.[101]

There is currently no uniform standard for the contents and form of blockchain voting rights, leading to considerable heterogeneity between different blockchains. In general, voting rights in the blockchain rarely regard the appointment of agents or distributions,

---

95. For an example of the marketing efforts that accompany blockchain offerings, *see infra* notes 292–294 and accompanying text, which highlight Tezos's marketing initiatives during its ICO.

96. Shaanan Cohney et al., *Coin-Operated Capitalism*, COLUM. L. REV. (forthcoming 2018) (manuscript at 18), https://ssrn.com/abstract=3215345.

97. *Id.* at 6.

98. *See infra* Section IV.D (providing examples of the different groups offering blockchain units).

99. *See infra* Section IV.D.2 (describing how Tezos's ICO was designed as a fundraiser for a non-profit organization).

100. The DAO, discussed in detail below, is one example of an unincorporated organization offering tokens. *See infra* Section IV.A.2.

101. *See, e.g.*, Rohr & Wright, *supra* note 85, at 22–23 (describing the different rights that different blockchains provide to their holders, which may include certain governance rights depending on the type of blockchain).

but typically consist of direct decision making in the underlying assets represented by the tokens.[102] Some blockchains offer their unit holders voting rights on a variety of questions. According to a recent study, "nearly 25[percent of tokens] provide some sort of governance rights, like voting on decision polls."[103]

In addition, because most blockchain-based assets are embedded in open software, users can "fork" the code and lead the blockchain to a different direction from that chosen by the lead developers, building an alternative blockchain that mimics the rules of the original but has certain modifications.[104]

Other voice mechanisms vary by asset. For example, in Bitcoin, the voice option is technically embedded in a process called "Bitcoin Improvement Proposals" (BIP),[105] whereas in any open source project, anyone can propose changes to the blockchain, coordinate a discussion of their merits, and attempt to build a consensus in the community in favor of implementing the proposal.[106] BIPs are a feature of decentralized ledger offerings that are generally not available in centralized entities with centralized software and management.

II. EMBEDDED COSTS AND RISK FACTORS IN BLOCKCHAIN-BASED ASSETS

This Section identifies unique costs and risk factors affected by the blockchain technology. While every blockchain-based asset has an idiosyncratic functional value and is pitched to potential investors with an anticipation to deliver particularly innovative products or

---

102. *See Bitcoin Improvement Proposals*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals (last visited Oct. 17, 2018) (explaining the process through which decisions are made with respect to blockchain-based assets because Bitcoin has "no formal structure" for voting on proposed changes).

103. CARDOZO BLOCKCHAIN PROJECT, *supra* note 9, at 2.

104. *See* NARAYANAN ET AL., *supra* note 16, at 171.

105. *Bitcoin Improvement Proposal (BIP)*, INVESTOPEDIA, https://www.investopedia.com/terms/b/bitcoin-improvement-proposal-bip.asp (last visited Oct. 17, 2018) ("The Bitcoin Improvement Proposal (BIP) is a formal design document that outlines the technical details and rationale for the features and changes to be introduced to the bitcoin network.").

106. Peter Van Valkenburgh, *What Is "Open Source" and Why Is It Important for Cryptocurrency and Open Blockchain Projects?*, COIN CTR. (Oct. 17, 2017), https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects ("Open source software is collaboratively produced, shared freely, published transparently, and developed to be a community good rather than the property or business of a single company or person.").

technologies, blockchain-based assets share several embedded costs and risk factors as an asset class, affected by their technology and economic structure. The following analysis describes four of these embedded costs and risk factors and draws attention to their unique manifestation on the blockchain: controlling costs, monitoring costs, systemic risks, and technology risks. Drawing attention to specific costs and risk factors inherent to blockchain-based assets enables a more concrete assessment of their potential regulation as securities.

A. Controlling Costs

Controlling costs are the costs the investor incurs from the behavior of a party that is positioned with sufficient influence to exert control on the blockchain, i.e., the entrepreneur, issuer, intermediary offering the tokens, or any person in a position to significantly maneuver the blockchain business and its operation.[107]

Controlling costs are an important source of blockchain agency costs, and include potential self-dealing, which diverts value from the blockchain. This is typically manifested in transactions between the controller and the blockchain, transactions where value is transferred from a particular blockchain holder to other businesses held by the controller,[108] other tunneling efforts, and lastly, fraud and misuse of funds by the controller. Assessment of the prevalent controlling costs of any particular blockchain-based asset in question is of critical importance for the purpose of assessing the potential value of regulating it as a security. In the absence of controlling costs, in its pure decentralized form, the pivotal justification for securities regulation dissolves: there are no informational asymmetries when no party is positioned to influence and benefit from the blockchain more than another, and there could be no expectation or reliance on the managerial efforts of such controller and her performance.

In theory, decentralized blockchain technology can create and cultivate assets for public investors without the traditional externalities of agency costs. Blockchain technology allows for exchange and transfer of property rights without relying on an intermediary, replacing the traditional controller or issuer with a computing process

---

107. *See* Lucian A. Bebchuk & Assaf Hamdani, *The Agency Costs of Controlling Shareholders* 6 (2018) (unpublished manuscript), https://www.jstor.org/stable/4126740?seq=1#metadata_info_tab_contents.

108. For an analysis of indirect tunneling, see *id.* at 14–15.

forming a consensus protocol within a network of nodes or users.[109] The decentralized ledger technology implies that not all blockchains have a controller.[110] For example, Bitcoin is a cryptocurrency that relies on a broad community of miners to expand and prosper, replacing the traditional issuer with a network of dispersed users.[111]

Yet, reality is more complicated, and offerings of blockchain-based assets have varied degrees of controlling costs. Assessing controlling costs in a decentralized ledger requires a structural assessment of the technical properties of the blockchain to see whether any particular agent or party is positioned to influence the ledger and its performance so as to (1) maneuver its business and operating functionality, and (2) potentially divert value from holders of blockchain-based assets (tokens or cryptocurrencies) towards the agent or party or any affiliate. Blockchain investors should ask, hypothetically, whether any particular party could potentially exert control on the blockchain, and whether such control could carry costs (e.g., by self-dealing or indirect tunneling) and thereby potentially abuse the trust of token holders.

Assessing the ability to maneuver a blockchain-based asset is harder than assessing the ability to maneuver a traditional corporation. Unlike traditional corporations, where control is legally defined and represented in shared ownership, control over a blockchain-based asset is highly technical and elusive. Controllers of blockchain-based assets do not necessarily share a limited pool of resources with other owners of the blockchain's units because often the supply of blockchain-based units is infinite—or effectively infinite.[112] Assessing the degree of control over a blockchain-based asset requires technical evaluation of a controller's effective influence over the operating functionality of the blockchain-based asset. Some blockchain-based assets are operating on a centralized technology. For example, the recent ICO of Iota, a decentralized ledger offering a cryptocurrency of

---

109. *See* Rohr & Wright, *supra* note 85, at 87 (explaining that "[b]lockchains are, at their core, a technology that renders . . . intermediaries . . . largely unnecessary" due to the function of smart contracts).

110. William Hinman, Director, Div. of Corp. Fin., U.S. Sec. & Exch. Comm'n, Remarks at the Yahoo Finance All Markets Summit: Crypto (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.

111. For a detailed discussion of potential controlling costs in Bitcoin, see *infra* Section IV.

112. *See supra* note 66 and accompanying text (discussing limited money supply in blockchain-based assets); *see also* Cohney et al., *supra* note 96, at 33 (documenting a lack of supply controls in initial coin offerings based on a 2017 survey).

the internet of things, pitched itself as a decentralized ledger, yet technically directed through a coordination node run through the Iota foundation.[113] Similarly, cryptocurrency Ripple is widely considered a service running on centralized servers.[114]

Yet, in blockchain-based assets using a decentralized ledger as their platform, the ability to maneuver the blockchain is harder to infer. After all, each node—or holder—of the blockchain-based asset can voluntarily decide whether or not to follow the controllers' recommendation, and the software itself is typically open source and can be easily duplicated.[115] Some instances where control can be manifested are protocol enhancement and security incident responses (e.g., responses to cybersecurity violations in the protocol or software, theft of tokens, etc.). Many blockchain-based assets have a group of developers that enjoy a status of reputable leadership in the blockchain community so as to influence holders of units of the blockchain-based asset to voluntarily accept its recommendations and perform software upgrades and/or fork according to the leadership's recommendation.[116] Such influence can be full or partial, but is rarely exclusive or binding.[117]

Assessment of controlling costs requires identification of controlling parties possessing the technical ability to maneuver the blockchain, with potential diversion of value from holders of units of the blockchain-based asset to the controller(s). The ledger can be technically decentralized, with controlling costs subtly embedded in the original allocation of tokens of the blockchain, or through its code. For example, some blockchains are offered to the public with a time-lag delay that is designed to allow the offeror time to conduct "pre-mining" with lower costs, effectively preceding the decentralized process with a centralized one, granting the controller privileges.[118] Controlling costs can also arise from colluding miners on a decentralized ledger.

---

113. *See* Eric Wall, *IOTA is Centralized*, MEDIUM (June 14, 2017), https://medium.com/@ercwl/iota-is-centralized-6289246e7b4d.

114. *See* Jamie Redman, '*So Wait—Is Ripple Centralized After All?*,' BITCOINIST (Dec. 15, 2015, 10:01 AM), http://bitcoinist.com/wait-ripple-centralized.

115. *See supra* Section II.C.2 (providing an overview of language and form).

116. *See About the Ethereum Foundation*, ETHEREUM, https://ethereum.org/foundation (last visited Oct. 17, 2018) (stating that Ethereum's mission includes empowering developers and, more generally, working with developers to enhance the blockchain community).

117. This is because each node can choose whether to install the recommended update and/or whether to follow the fork or not. The leadership of a decentralized ledger is not in position to enforce its recommendation other than by voluntary compliance.

118. *See* Madeira, *supra* note 59.

Bitcoin miners could obtain revenue larger than their fair share by colluding, implying that rational miners will prefer to join the selfish miners, and the colluding group could potentially increase in size until it becomes a controlling majority.[119]

To illustrate the prevalence of controlling costs diverting value from investors to controllers on a decentralized ledger, consider the examples of Confido, Iota, and DAO, all ICOs from 2017. Confido, a startup on the Ethereum platform, vanished from the internet after raising $374,000 from investors in an ICO fundraiser, having pitched itself as a blockchain-based application for making payments and tracking shipments.[120] A few days after the offering, Confido deleted its Twitter account and took down its website, leaving the raised amount in the hands of its controllers.[121] Another example is the DAO, a case investigated by the SEC and thoroughly reviewed in this Article.[122] In this case, self-dealing was evident as DAO's originator, Slock.it, announced it would be the first to submit a proposal for funding by the blockchain's platform, effectively awarding itself a financial grant for another business it owns at the expense of DAO's token holders.[123]

B. Monitoring Costs

Different blockchains have different lengths of chain separating the original cash producing asset from the ultimate investor with economic rights to cash flows stemming from that asset.[124] A structural assessment of the blockchain is required to measure the placement of the cash producing asset, both in terms of the length of the contractual chain separating it from the ultimate investors and in terms of the ability of automation platforms embedded in the blockchain to verify performance, thereby reducing uncertainty and potential

---

119. Ittay Eyal & Emin Gün Sirer, *Majority is Not Enough: Bitcoin Mining is Vulnerable*, CORNELL U. DEP'T COMPUT. SCI., https://www.cs.cornell.edu/~ie53/publications/ btcProcFC.pdf.

120. Jordan Pearson, *An Ethereum Startup Just Vanished After People Invested $347K*, VICE (Nov. 20, 2017, 1:27 PM), https://motherboard.vice.com/en_us/article/j5j34x/ethereum-startup-confido-vanished-after-people-invested.

121. *Id.*

122. *See infra* Section IV.A.2.

123. For the SEC report on the DAO, *see infra* note 225.

124. *See Bitcoin vs Ethereum*, *supra* note 66 (comparing Bitcoin and Ethereum to illustrate how different blockchains have different lengths of chain, which ultimately results in different transaction speeds).

manipulation.[125] Monitoring costs have a pernicious effect on the ability of investors to evaluate their investment's merit ex ante and to assess its performance ex post. Therefore, a thorough understanding of costs should be a key factor is assessing the adequacy of the potential securities regulation of the blockchain.

In some blockchains, the underlying sources of value can be verified automatically on the blockchain, while other blockchains require off-chain verification.[126] In the latter cases, an exogenous performance of an underlying value source, such as real economic assets, products, services, indices, commodities, or technologies, are attached to the token and are virtually represented by the blockchain's units.[127] As derivative contracts, tokens can represent value in an underlying market sphere, and thus their holders are exposed to shifts and movements in that underlying market. When the value of the token is on-chain, the blockchain technology offers an automated verification process for the exchange forming the transaction.[128] Either the value is intrinsic to the token itself, as is the case with Bitcoin, or the value is extrinsic to the token but can still be verified automatically on platforms attached to it.[129] However, when the value attached to the token is off-chain, the automatic verification protocols of the blockchain are insufficient—monitoring cannot be automated. Monitoring costs of the value underlying the blockchain will be particularly high when the value represented by the blockchain is vague, cannot be verified automatically, or when the underlying value has to do with off-chain entities and expected future performances.

---

125. *See* O'Shields, *supra* note 91, at 179 (discussing the beneficial role of smart contracts, which reduce uncertainty and potential manipulation by ensuring that agreements are properly executed and enforced in the blockchain).

126. *See Off-Chain Transactions*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Off-Chain_Transactions (last visited Oct. 17, 2018) (highlighting the key differences between off-chain and on-chain transactions in the context of blockchain-based assets).

127. *See supra* Section I.C.1 (considering the different sources of value attached to blockchain-based assets).

128. *But see On Chain Transactions (Cryptocurrency)*, INVESTOPEDIA, https://www.investopedia.com/terms/c/chain-transactions-cryptocurrency.asp (last visited Oct. 17, 2018) (asserting that on-chain transactions "rarely occur instantly" even though they are "supposed to occur in real time . . . to keep blockchain transactions . . . verifiable . . . and instantaneous").

129. John Kelleher, *What is Bitcoin's Intrinsic Value?*, INVESTOPEDIA, https://www.investopedia.com/articles/investing/091814/what-bitcoins-intrinsic-value.asp (last visited Oct. 17, 2018).

Monitoring the value of the blockchain's off-chain requires an expansion of the blockchain's automated capacities, giving rise to asymmetric information, opportunism, self-dealings, and other potential agency costs.[130] It is simply something the automated verification process of blockchain cannot yet do. When the value attached to the token is off-chain, monitoring the underlying value may require an intermediary or another established protocol for its continuous ongoing assessment.[131] Because on-chain values can be monitored through the automated blockchain protocol, and off-chain values cannot, the cost of monitoring exogenous values represented by tokens becomes costly and is prone to manipulation and misinformation.

To illustrate, consider the cases of Confido and DAO mentioned above.[132] In Confido, assessment of value had to do with monitoring the value of making payments and tracking shipments in Germany, the service Confido pitched itself with.[133] In the DAO case, assessment of value had to do with the changing value of the investments portfolio formed by the funded projects chosen by the blockchain enterprise.[134] Both missions cannot be verified automatically, and require an intermediary, an auditor, or some other agency to perform ongoing valuations for the performance of an off-chain enterprise.

Blockchains can employ a number of mechanisms to address the costs of off-chain monitoring. First, they may allocate property rights through the provision of actual assets to the token holders. For example, Filecoin provides its token holders with storage space, and uses replication parameters to protect against different threat models.[135] Second, blockchains may use a trusted third party to provide a guarantee for the data forming the underlying value, replacing the

---

130. *Understanding Off-Chain Transactions in Blockchain for Fun and Profit*, MEDIUM (Dec. 4, 2017), https://medium.com/@liquidity.network/understanding-off-chain-transactions-in-blockchain-for-fun-and-profit-591e7e27ccc0.

131. Thomas Jay Rush, *Decentralized, Off-chain, Per-block Accounting, Monitoring, and Reconciliation of Blockchains*, https://quickblocks.io/wp-content/uploads/2017/10/2017-Rush-Decentralized-Off-Chain-per-Block-Accounting-Monitoring-and-Reconciliation-for-Blockchains.pdf (last visited Oct. 17, 2018).

132. *See supra* Section IV.A.2.

133. *See supra* notes 119–122 and accompanying text.

134. *See supra* notes 120–123 and accompanying text.

135. The protocol's cloud storage network also provides security, as content is encrypted end-to-end by the client, while the storage providers do not have access to an encryption key.

traditional valuation agent.[136] Third, blockchains may use reputational incentive in cases where the offeror has, or plans to have, a history or a sequence of repeat transactions.[137]

C. Technology Risk

Blockchain technologies hedge against some risks and aggravate others. Due to blockchain technology, blockchain-based assets with decentralized ledgers are generally resilient to damages and interruptions from natural disasters such as earthquakes, terrorist attacks, computer viruses, and other catastrophes. As the decentralized ledger runs simultaneously on each node and every node also maintains it, damage to any particular node or small group of nodes does not disrupt the functioning of the ledger.[138]

However, encoding the investment contract on the blockchain poses risk for costly mistakes and hidden bugs impeding the blockchain's performance. Harm from a mistake or a bug in a blockchain-based asset cannot be undone by revoking the investment contract, and therefore exposes investors to cyber-attacks, interventions, and manipulations by third parties.[139] Unlike traditional contracts that are subject to enforcement by courts, smart contracts are technically immutable: automatically enforced according to their original code with no allowance for ex post discretion.[140] Automation inevitably makes smart contracts complete, despite their inevitable realistic incompleteness due to uncertainty, risks, and simple "bugs" and coding mistakes.[141] Thus, the costs of detecting the mistake and debugging the

---

136. *See, e.g.*, TOWN CRIER, http://www.town-crier.org (last visited Oct. 17, 2018) (showing an example of an authenticated data feed for smart contracts).

137. Vitalik Buterin, *Visions, Part 1: The Value of Blockchain Technology*, ETHEREUM (Apr. 12, 2015), https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology (discussing the value of reputation to the blockchain as a platform).

138. The consensus protocols used to maintain the ledger rely on some assumptions about the nodes, typically (in a blockchain based on proof-of-work consensus) that among the nodes participating in mining, at least half of the computational power belongs to nodes that behave honestly.

139. *See infra* notes 143–144.

140. *See* Mary Juetten, *Legal Technology and Smart Contracts: Blockchain and Smart Contracts (Part IV)*, FORBES (Sept. 6, 2017, 8:00 AM), https://www.forbes.com/sites/maryjuetten/2017/09/06/legal-technology-and-smart-contracts-blockchain-smart-contracts-part-iv (discussing how smart contracts are used to strictly enforce the contracts).

141. *See* PATRICK BOLTON & MATHIAS DEWATRIPONT, CONTRACT THEORY 36–37 (2005) (explaining that contracts may be incomplete since they cannot explicitly address all possible contingencies or future events); Charles J. Goetz & Robert E. Scott, *Principles of Relational Contracts*, 67 VA. L. REV. 1089, 1091 (1981); Oliver Hart & John Moore,

blockchain investment contract are very high. Investors are unlikely to reveal the information, given their relative stake in the transaction and collective action costs, and the seller has few incentives to do so, as debugging the smart contract ex ante does not necessarily increase seller profits. Because information regarding facts leading to a mistake is so scarce, in particular given the unique coding language used by each blockchain, it may make the most sense to assign the costs of a potential mistake to the seller, who is the cheaper information-gatherer.[142]

One example of the risks in "bugs" is the June 2016 cyber-attack on DAO, under which the attacker removed 3.6 million ETH, a third of the total raised by the DAO offering, from DAO's Ethereum blockchain to another Ethereum blockchain controlled by the attacker, utilizing a bug in the software of the DAO's smart contract.[143] The bug was an inseparable part of the contract between the DAO blockchain and the DAO token holders.[144] The bug was essentially a mutual mistake, an incorrect belief shared by both parties at the time of the offering about the contractual terms. While legal conventional wisdom about mutual mistakes as incorporated into the Restatement (Second) of Contracts[145] makes the contract potentially void,[146] automation of the contract on a blockchain makes avoidance technically impossible. Smart contracts are a "one-way train," technically unstoppable.[147]

Foundations of Incomplete Contracts, 66 REV. OF ECON. STUD. 115, 116 (1999) (discussing the challenges of incomplete contracting); Robert E. Scott & George G. Triantis, *Anticipating Litigation in Contract Design*, 115 YALE L.J. 814, 822–24 (2006). Unlike traditional incomplete contracting, which is an outcome of the high costs of predicting, understanding, and assessing the probabilities and the costs in different potential states of the world, a bug in the software running the blockchain is a complete form specifying the possibility of failure ex ante—contractually embedded in complex coding language.

142. Anthony T. Kronman, *Mistake, Disclosure, Information and the Law of Contracts*, 7 J. LEGAL STUD. 1, 4 (1978).

143. For the SEC's investigation report assigning the DAO as a security, see *infra* Section IV.A and note 225.

144. *See infra* Section IV.A.2; Report on Investigation, *infra* note 225, at 9.

145. RESTATEMENT (SECOND) OF CONTRACTS § 152(1) ("Where a mistake of both parties at the time of contract was made as to a basic assumption on which the contract was made has a material effect on the agreed exchange of performances, the contract is voidable by the adversely affected party unless he bears the risk of the mistake stated in section 154.").

146. E. ALLAN FARNWORTH, FARNSWORTH ON CONTRACTS 509, 520–21 (1990).

147. *See* Jeremy M. Sklaroff, *Smart Contracts and the Cost of Inflexibility*, 166 U. PA. L. REV. 263, 302 (2017) (suggesting that the rigid nature of smart contract interpretation is not always a good thing).

Eventually, in this case, and subject to their ad hoc ultimate discretion, developers of Ethereum led by Vitalik Buterin decided to voluntarily apply (with no legal or technical obligation) a "fork" into the Ethereum blockchain so as to create a new version of code with new rules for Ethereum that would rule out the attack and recreate a new version of the blockchain, where an alternative "better" universe exists and where the attack could not have occurred.[148] The fork undermines the decentralized vision of Ethereum and is essentially a form of a bailout given by the leadership of Ethereum ad hoc. There is no published governance procedure for making such future decisions, and clearly, they are not necessarily replicable.

The DAO fork had a double effect. First, in the new amended universe established by the fork, called "Ethereum Classic,"[149] holders of DAO tokens fully recovered their stolen funds, so despite the cyber-attack, holders of DAO could exchange their DAO tokens to Ether cryptocurrency issued by the Ethereum blockchain.[150] Second, the original Ethereum blockchain continues to run alongside Ethereum Classic, and in it, the attackers still have access to the stolen funds. As a result of the fork, both the attacker and the holders of DAO tokens can exchange tokens to ETH and then to USD.

The case of the DAO/Ethereum fork demonstrates the complexity of applications of blockchain technology to the financial services sector. Automation makes property rights crystal clear, but exposes them to bugs and other mistakes on a rigid platform with zero ex post flexibility.[151] A bug in the code discovered along the course of business can only be remedied by a platform-wide amendment, exposing investors to the ultimate discretion of the platform leadership, if one exists, while also

148. Francis Coppola, *A Painful Lesson for the Ethereum Community*, FORBES (July 21, 2016, 1:54 PM), https://www.forbes.com/sites/francescoppola/2016/07/21/a-painful-lesson-for-the-ethereum-community ("The fact is that Ethereum has compromised its principles in order to rescue a client. Or, in the language of another world, the Ethereum central bank has directly recapitalized the DAO commercial bank by monetizing its debts.").

149. *See generally* Antonio Madeira, *What is Ethereum Classic*, CRYPTOCOMPARE (Oct. 4, 2018), https://www.cryptocompare.com/coins/guides/what-is-ethereum-classic; *Ethereum Classic*, INVESTOPEDIA, https://www.investopedia.com/terms/e/ethereum-classic.asp (last visited Oct. 17, 2018).

150. Antonio Madeira, *The DAO, The Hack, The Soft Fork and the Hard Fork*, CRYPTOCOMPARE (July 30, 2018), https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork.

151. *Managing the Risks of Blockchain*, BANKING TECH (Mar. 6, 2018), https://www.bankingtech.com/2018/03/managing-the-risks-of-blockchain.

giving rise to systemic financial stability concerns due to a new form of quantum financial institution, where financial assets can be duplicated, recreated and co-exist simultaneously within two ends of the fork.[152]

D. Systemic Risk

Blockchain-based assets impede transparency and contractual flexibility in ways that potentially increase widespread financial distress in the markets, defined in the literature as a systemic risk.[153]

Financial crises are often preceded by a bubble in which one or more classes of assets are traded at prices far in excess of their fundamental values.[154] The accuracy of price signals depends in part on the presence of informed traders in the relevant marketplace.[155] The lack of sufficiently informed traders can increase the amount of noise surrounding the price signals created in that market.[156] When over-excitement and over-optimism are added, the noise tends to skew price signals and creates an environment in which it is easier for a bubble to develop.[157] Blockchain offerings are inherently structured to reflect such an environment. The nature of the blockchain offering requires a translation from code to English to assess the terms of the investment, making the contract effectively indecipherable for many (if not most) investors. While no empirical profiling of blockchain investors has been published, the lack of institutional representation in the blockchain territory suggests that at least some of that value acceleration stems from investors who have limited ability to assess the quality of the

152. *See* Coppola, *supra* note 148.

153. Hal S. Scott, *Reducing Systemic Risk Through the Reform of Capital Regulation*, 13 J. INT'L ECON. L. 763, 763–64 (2010).

154. Martin Neil Baily et al., *The Origins of the Financial Crisis*, BROOKINGS (Nov. 24, 2008), https://www.brookings.edu/research/the-origins-of-the-financial-crisis.

155. Ronald J. Gilson & Reinier H. Kraakman, *The Mechanisms of Market Efficiency*, 70 VA. L. REV. 549, 570 n.67 (1984).

156. *Id.* at 578.

157. Minsky's instability hypothesis posits that the inherent instability of the financial system is driven by the frequency and amplitude of investments made, based on lender assessment rather than aggregate value.

assets underlying their investments.[158] Bitcoin, for example, has risen within eight years to a total market capitalization of $138 billion.[159]

Another cause of concern that is often overlooked is manifested by "forks" in the blockchain platform, essentially printing an alternative mirrored universe of money, with dubious value.[160] The technical triviality of duplicating entire crypto currencies with their user network in a world where almost all software is open sourced raises a concern. Consider the examples of duplicating Bitcoin's network with a fork, discussed above.[161] After years of debate among Bitcoin holders about the limited scale of the Bitcoin, a group of Bitcoin holders copied Bitcoin's code and applied it on an alternative blockchain, and simultaneously copied all of the Bitcoin owners' data and granted them respective rights in the new alternative blockchain (free of charge), effectively copying Bitcoin's entire network and applying it on an alternative blockchain.[162] This move resulted in the creation of Bitcoin Cash,[163] a rival cryptocurrency that is similar to Bitcoin but touts a far larger block size. As a result of the fork, Bitcoin holders passively became simultaneous holders of both Bitcoin and Bitcoin Cash, two clone cryptocurrencies, each with its own rates of return,

158. The fast acceleration in value has led many to consider ICOs and other blockchain offerings "unmasked as scams and Ponzi schemes" touched with "observable overexcitement." Dirk Zetzsche et al., *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators* 12 (Paper No. 2017-011, 2018), https://ssrn.com/abstract=3072298. *See generally* HYMAN P. MINSKY, CAN "IT" HAPPEN AGAIN?: ESSAYS ON INSTABILITY AND FINANCE 9 (1982). My question refers to infrastructure securitization and the Great Recession following the 2007-2009 financial crisis and does not analyze characteristics of other financial crises. *See* Jeffrey N. Gordon & Christopher Muller, *Confronting Financial Crisis: Dodd-Frank's Dangers and the Case for a Systemic Emergency Insurance Fund*, 28 YALE J. ON REG. 151, 167 (2011).

159. As of November 24, 2017. Calculated as the number of tokens in circulation times the value of each token. The second largest cryptocurrency, Ethereum, has a $30 billion market cap. *See Top 100 Cryptocurrencies by Market Capitalization*, COIN MARKET CAP, https://coinmarketcap.com (last visited Oct. 17, 2018).

160. Sometimes, blockchain forks represent actual sources of value, amending the original code source in a significant way. Other times, the forks are simply a bailout mechanism internal to the platform that allows an effective method to increase the quantity of money analogous to printing money by central banks.

161. *See supra* notes 46–48.

162. *See* David Glance, *Bitcoin Splits and Bitcoin Cash is Created: Explaining Why and What Happens Now*, THE CONVERSATION (Aug. 1, 2017, 10:05 PM), http://theconversation.com/bitcoin-splits-and-bitcoin-cash-is-created-explaining-why-and-what-happens-now-81943.

163. *Id.*

fluctuations, and technical specifications. The new currency is added as an additional asset on top of holders' stake in the original blockchain.

Blockchain offerings pose a systemic risk for a third reason: their rigidity and "stickiness." Stickiness refers to contractual "arrangements [that] are exceptionally difficult to modify."[164] Contractual rigidity and stickiness increase the likelihood that any particular loan would be foreclosed because renegotiation is less likely and incurs significant costs.[165] When contractual rigidity and stickiness are widespread phenomena across a market, their accumulated effect may lead to systemic risk.[166] Contractual rigidity and stickiness were shown to increase systemic risks in the 2007–2009 financial crisis.[167] In blockchain territory, stickiness and contractual rigidity are inevitable. In a recent application of Ronald Gilson, Charles Sabel, and Robert Scott's work on braiding to blockchain territory,[168] Jeremy Sklaroff has argued that blockchain-based assets impede both the semantic flexibility and the enforcement flexibility of traditional contracts.[169] Semantic flexibility comes from the inherent ambiguity of human language. In traditional contracts, performance standards, such as "good faith" or "commercially reasonable," are critical tools for parties contracting in uncertain or volatile environments. Ambiguous contractual language postpones interpretation of a term until there's more information about the parties' performance, lowering the costs of negotiation and drafting. It also shifts those costs to the enforcement stage of the contracting process, where a court applies interpretation rules to give substance to the term.[170] Yet, blockchain-based assets are embedded in code, a binary language leaving no room for ex post interpretation. Likewise, as illustrated above, automation

---

164. Kathryn Judge, *Fragmentation Nodes: A Study in Financial Innovation, Complexity, and Systemic Risk*, 64 STAN. L. REV. 657, 700–03 (2012).

165. *Id.* at 704–05.

166. *Id.* at 709.

167. Loans packaged into securitized polls were less likely to be renegotiated and amended, compelling enforcement despite high externalities due to high coordination costs. As some researchers vividly pointed out, "when such rigid contracts are ubiquitous, they can function as social suicide pacts." Anna Gelpern & Adam J. Levitin, *Rewriting Frankenstein Contracts: Workout Prohibitions in Residential Mortgage-Backed Securities*, 82 S. CAL. L. REV. 1075, 1075 (2009).

168. *See generally* Ronald J. Gilson et al., *Text* and *Context: Contract Interpretation as Contract Design*, 100 CORNELL L. REV. 23, 26 (2014); Robert E. Scott et al., *Braiding: The Interaction of Formal and Informal Contracting in Theory, Practice, and Doctrine*, 110 COLUM. L. REV. 1377 (2010).

169. Sklaroff, *supra* note 147.

170. Gilson et al., *supra* note 168, at 42.

on a blockchain makes avoidance and amendment technically impossible, impeding the enforcement flexibility of blockchain investment contracts as well.[171] Blockchain-based assets are inevitably rigid and "sticky" and may therefore increase systemic risk because no party has the discretion to amend them, even if so desired. Yet, securities regulation is not a suitable instrument to address stickiness as an independent source of systemic risk. Mandatory disclosure cannot create contractual flexibility on the blockchain.

Finally, assessment of systemic risks has to do with the degree of interconnectivity of the subject of concern. Bank failure is considered a mega-economic event because when banks go down, many other parts of the real economy go with them, whether due to a heavy contractual chain of commitments, derivatives trading, and/or a simple downturn of the short-term debt supply.[172] With most blockchain-based assets, as of 2018, such interconnectivity is still minimal, trading volumes are rather low, and there is not much contractual activity between the blockchain space and the real economy. If a blockchain goes down in 2018, it is hard to see how the entire economy would be affected, and how other segments of the economy would be curtailed. Yet, the degree of interconnectivity of a blockchain-based asset is a potential source of systemic risk, and as argued below, should be evaluated on a case-by-case basis by regulators considering the blockchain's potential regulation as a security.[173]

III. JUSTIFICATION FOR SECURITIES REGULATION OF BLOCKCHAIN-BASED ASSETS

This section builds upon the descriptive foundations of the preceding parts and merges the unique properties of blockchain-based assets, embedded costs and risk factors, and theorizes about when securities regulation is warranted. Major theoretical justifications for securities regulations are reviewed, shedding light on when securities regulations of blockchain-based assets are theoretically warranted. According to the Securities Act, an offer or sale of securities to the public must be accompanied by a full and fair disclosure, enabling

171. *See* Sklaroff, *supra* note 147 and accompanying text (noting the inherent challenges in amending contracts automated on blockchain).

172. *Cf.* JOHN ARMOUR ET AL., PRINCIPLES OF FINANCIAL REGULATION 3–4 (2016).

173. *See infra* notes 201–205 and accompanying text.

potential purchasers to make an informed investment decision.[174] This vision of transparency is afforded by mandatory registration with the SEC and requires, *inter alia*, delivery of a statutory prospectus informing purchasers about the issuer's financial statements, management, business, and price and the amount of securities to be offered.[175] Securities include "investment contracts," defined as investments of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.[176] For any investment that is not in a form of cash, the question arises whether an investment contract exists.

A. Mandatory Disclosure

The impetus of the mandatory disclosure is to remove the information asymmetry between investors and offerors so as to promote informed investment decisions. According to the conventional wisdom, mandatory disclosure afforded by securities laws holds the promise to enhance price accuracy and thereby accommodate value maximization of firms for their owners.[177] In the absence of disclosure costs and if purchasers know that firms have a given piece of information and deem it relevant to their decision, a firm is theoretically expected to reveal all its information.[178] Even in the presence of disclosure costs, sellers offering blockchain-based assets or "tokens" have good incentives to voluntarily disclose its properties as a means of differentiating their own tokens from others

---

174. 15 U.S.C. § 77(a)–(c) (2012) (prohibiting the sale or offer to buy securities unless a registration statement has been filed; also prohibiting unregistered offerings); SEC v. Universal Major Indus. Corp., 546 F.2d 1044, 1047 (2d Cir. 1976) (holding that violations of § 5 do not require scienter).

175. 15 U.S.C. § 77(f)–(g), (j) (2012); SEC v. Cavanagh, 1 F. Supp. 2d 337, 360 (S.D.N.Y. 1998).

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

177. Allen Ferrell, *Measuring the Effects of Mandated Disclosure*, 1 BERKELEY BUS. L.J. 371, 372 (2004).

178. This result is rooted in the assumption of perfect functioning of information markets. If prices fully reflect quality, sellers have the incentive to disclose information about product quality so that they can charge an adequate price for their product. In the absence of such disclosure, consumers will not pay the designated price since they would assume the worst about the product's value. Thus, sellers, except those offering the lowest quality, have an incentive to voluntarily disclose information regarding their product. If disclosure is costly, sellers are expected to voluntarily disclose only if their quality exceeds a threshold. Sanford J. Grossman, *The Informational Role of Warranties and Private Disclosure About Product Quality*, 24 J.L. & ECON. 461, 461 (1981); W. Kip Viscusi, *A Note on "Lemons" Markets with Quality Certification*, 9 BELL J. OF ECON. 277, 279 (1978).

available on the market. If the offering does not disclose token information, the offeror will not be able to charge extra for the additional quality provided. This is because in the absence of information about product differentiation, purchasers are expected to assume a similar level of quality for competing products. Therefore, sellers of above-average products have an incentive to disclose further information, distinguishing their products from the lower-quality competitors.[179] Theoretically, this scenario may result in a reversed "lemon" process[180]—if purchasers assume non-disclosing sellers are offering lower quality products, more and more sellers would disclose to associate themselves with higher quality products. With more sellers disclosing, the process would repeat itself until all types, except the lowest, are disclosed. Such a process is expected to lower the average percentage of non-disclosing sellers, until every seller discloses.[181] If informed consumers reach a critical mass, sellers in a sufficiently competitive market will have an incentive to cater to the needs of these informed buyers and thus confer benefits to the non-informed consumers as well.[182]

Disclosure is not likely to stem voluntarily when investors are of diverse backgrounds and lack the technical expertise required to assess the terms of the offering. When purchasers fail to understand sellers' disclosures, disclosure is less likely to stem voluntarily. Under such conditions, sellers of higher quality products will not be able to distinguish themselves from sellers of lower quality products, and low-quality sellers will have incentives to hide their quality.[183] Conversely,

---

179. *See* Howard Beales et al., *The Efficient Regulation of Consumer Information*, 24 J.L. & ECON. 491, 502 (1981).

180. *See generally* Viscusi, *supra* note 175.

181. *See* Grossman, *supra* note 178, at 465. This analysis considered in itself implies that regulatory intervention in disclosure is completely unnecessary as eventually all sellers would disclose in order to signal quality. It is also backed up by some empirical works: George Benston, for example, compared the pre- and post-legislation disclosure made by firms prior to the 1934 Securities Regulation reform, finding that no significant price effect resulted from the new mandated disclosure and concluding that voluntary disclosure prior to the act was sufficiently efficient. *See* George J. Benston, *Required Disclosure and the Stock Market: An Evaluation of the Securities Exchange Act of 1934*, 63 AM. ECON. REV. 132, 144–45 (1973).

182. *See generally* Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630 (1979).

183. This scenario is typically called market for lemons, since the marketplace rule applied here creates a race to the bottom on product quality: no seller has incentives to invest in higher quality products when higher quality cannot translate to higher prices. *See generally* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 QUARTERLY J. OF ECON. 488, 488 (1970).

when all investors are sophisticated, the reasoning for mandatory disclosure weakens, and offerors have better incentives to voluntarily disclose information to signal their competitiveness.

Thus, the identity of investors and their ability to fend for themselves is key to the assessment of a contract's status as a security. Investors of blockchain-based assets should be literate in code and have sufficient degree of technical proficiency to assess the terms of their investment and translate product knowledge into quality and price. Code, almost by definition, is complex and technical, but it is not indecipherable. In blockchain settings, it is typically open source and available for inspection. Investors who have the technical and/or financial resources to read the blockchain's code can fend for themselves and do without the protection of securities regulation. Securities regulation can bring value in reducing the cost of information asymmetry for main street investors. Yet, as of 2018, investment in blockchain-based assets requires a rather high degree of technical and/or financial sophistication. Traditional financial intermediaries generally do not offer crypto investments off the shelf, and some consider it a threat.[184] Investors who are not tech savvy, or lack access to those who are, face a significant entry barrier to blockchain territory.

B. Standardization

Securities regulation is not only a means of mandatory disclosure, it is also a means to impose a mandatory uniform platform for information management. In many cases, voluntary disclosure means little without a backdrop for comparison of the underlying product whose features are disclosed. Take the securities market as an example. A company's statement as to its expected return on investment is meaningless without a standardized measure of industry or market performance that a potential investor can benchmark against. For this reason, securities regulation provides mandatory uniform conventions for financial statements, and sees this mandatory uniform convention as central to its purpose.[185] Raw data provided out of context is not very helpful.

---

184. David Floyd, *Bank of America, JPMorgan Call Cryptocurrencies a Threat*, INVESTOPEDIA (Feb. 28, 2018, 11:12 AM), https://www.investopedia.com/news/bank-america-calls-cryptocurrencies-risk-its-business.

185. Sharon Hannes, *Comparisons Among Firms: (When) Do They Justify Mandatory Disclosure?* 29 J. CORP. L. 699, 702 (2004) (quoting CLYDE P. STICKNEY & ROMAN L. WEIL, FINANCIAL ACCOUNTING 249 (10th ed., 2003)) ("This comparative advantage of disclosure, however, was never emphasized by the legal scholarship that dealt with the

Without mandatorily imposed standards of disclosure, as securities regulations provide, every seller would disclose in his own terms, language, and format, leading to market dynamics in which sellers would have no credible disclosure capacity or technology, and insufficient public quality assurances. Under such dynamics, as Akerlof's model of market for lemons suggests, only the average quality of the goods will be considered and fairly priced by consumers, and above-average quality products will be eventually driven out of the market.[186]

To enhance standardization, securities laws created a mandatory disclosure regime.[187] Disclosed information under securities laws has to fit the same patterns and be provided by the same metrics by all disclosing parties. The SEC collects all the submitted disclosures and posts them on its centralized website, EDGAR.[188] The standardization function of securities regulation requires exclusivity, so that free speech and other promotional media of expression are not permitted.

C. Investor Vulnerability

Securities laws were introduced in the 1930s to restore retail investors' trust in capital markets.[189] Reliable standardized mandatory disclosures are generally considered to enhance this trust, and thereby improve market participation.[190] Without regulatory intervention, markets

---

mandatory disclosure system. The absence of an inquiry into the nature of these benefits is odd, since at first glance the comparative benefits of disclosure, if they are indeed essential for the welfare of the capital markets, seem like a good justification for mandated disclosure.").

186. *See* Akerlof, *supra* note 183.

187. One such mandatory disclosure manifests in Regulation FD ("Fair Disclosure"). 17 C.F.R. § 243.100–.103 (2011). *See generally* Allen Farrell, *The Case for Mandatory Disclosure in Securities Regulation Around the World* (Harv. John M. Olin Ctr. for L., Econ., and Bus., Discussion Paper No. 492), http://www.law.harvard.edu/programs/olin_center/papers/pdf/Ferrell_492.pdf.

188. EDGAR, U.S. Sec. & Exch. Comm'n, http://www.sec.gov/edgar.shtml (last visited Oct. 17, 2018).

189. As Professor Donald Langevoort explains:

> [T]hroughout the SEC's history and culture, the rhetorical stress has been on the plight of average investors, ones who lack investing experience and sophistication so as to need the protection of the securities laws . . . The subsequent history of rules, interpretations, and enforcement by the SEC is filled with references to both the need to promote retail-level investor confidence . . . and the desire to level the playing field between the meek and the privileged.

Langevoort, *supra* note 15, at 1025–26.

190. Luigi Zingales, *The Future of Securities Regulation*, 47 J. OF ACCT. RES. 391, 391 (2009).

are unlikely to yield efficient levels of trust, both because rationally, incentives to collect information by each investor are suboptimal,[191] and behaviorally, investors are subject to psychological distortions and biases that will leave their knowledge below the desired level.[192]

One example for how securities laws cater to the needs of vulnerable investors is the "plain English requirement."[193] According to Securities Act Rule 421(d), issuers of securities are required to provide on the inside front and outside back cover of a prospectus, a summary of the offering and a discussion of the most significant risk factors that make the offering speculative or risky, detailed in plain English.[194] Rule 421(b) provides further guidance on how to prepare a prospectus to meet the preexisting rule that a prospectus be "clear, concise and understandable."[195] Together, these rules provide that disclosure under securities laws be accessible and comprehensible to vulnerable investors. To simplify complex information, disclosures are to be given in short sentences, in definite concrete and everyday language, in tabular presentation or bullet lists whenever possible, and with no legal jargon.[196]

With blockchain-based assets, the terms of investment are typically embedded in code, and while theoretically, purchasers can view the code, they are rarely in a position to assess its contents due to the highly complex and technical language. Literacy in coding language requires technical training, and even for those who possess skill, coding languages vary from one blockchain to another and require technical versatility from their readers. The identity of investors and their ability to fend for themselves is a critical test for the applicability of securities regulation.

D. Corporate Governance

The fourth generic justification for mandatory disclosure is based on its effect on the firm's governance. As Louis Brandeis famously stated in 1913, "[s]unlight is said to be the best of disinfectants."[197] Brandeis

---

191. *See* Oren Bar-Gill & Elizabeth Warren, *Making Credit Safer*, 157 U. PA. L. REV. 1, 69 (2008) (proposing that safety regulations are needed to help restore the market).

192. *See* John Y. Campbell, *Household Finance*, 61 J. FIN. 1553, 1554 (2006) (describing the collective action problem in the mortgage market that prevents sellers from educating consumers).

193. 17 C.F.R. § 229.503 (2011).

194. *Id.*

195. U.S. SEC. & EXCH. COMM'N, A PLAIN ENGLISH HANDBOOK: HOW TO CREATE CLEAR SEC DISCLOSURE DOCUMENTS 65 (1998).

196. *See id.* (describing the presentation guidelines for Rule 421(b)).

197. Brandeis's famous idiom appeared first in *Harper's Weekly* in a piece recommending a legal requirement for public companies to disclose their profits and

argued that transparency would create incentives for better ex ante performance and would transform corporate reality by virtue of making it transparent.[198] As shown by Professor Lucian A. Bebchuk, asymmetric information at the time of the offering indeed distorts corporate governance structures adopted voluntarily, leading to the adoption of corporate arrangements that are commonly known to be inefficient.[199]

When there is a person or organization performing an essential function critical to the success of the enterprise, mandatory disclosure is required to allow investors to assess the knowledge, performance, and financial stakes of that person or organization, both in the normal course of business and as a means of aligning the controllers' incentives with those of investors, mitigating agency costs and potential private benefits.[200]

Mandatory disclosure can also serve as a regulatory mechanism for verification and monitoring which may fill the monitoring function for purchasers when the automated platform of the blockchain is ill-equipped to execute the monitoring task, in particular when the value underlying the blockchain-based asset is off-chain.

E. Systemic Risks

In the division of labor between regulatory agencies, monitoring systemic risks is typically considered the responsibility of the financial sector regulators. Securities regulation, in comparison, is traditionally concerned with investor protection and efficient market functioning.[201]

Yet, informational asymmetries in the blockchain territory may warrant securities regulation. Mandatory disclosure can serve as a mechanism for reliably keeping prices tied to underlying values, a pertinent cause of concern with current blockchain offerings often described as an asset bubble.[202] As we learned from previous financial crises, the risk of

---

losses as a means to end deception by insider trading. While advocating for Securities Regulation, Brandeis pointed to the earlier 1906 Pure Food and Drug Act, which required listing of ingredients on interstate shipments of foods as a model of sunlight as a means to mitigate public risks. *See* LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914).

198. *See id.* at 103 (noting that the law should require full disclosures to consumers).

199. Lucian A. Bebchuk, *Asymmetric Information and the Choice of Corporate Governance Arrangements* 1, 26 (Harv. John M. Olin Ctr. for L., Econ., & Bus., Paper No. 398, 2002).

200. *See* Zingales, *supra* note 190, at 394–95 (describing the benefits and costs of mandatory disclosure).

201. Anita I. Anand, *Is Systemic Risk Relevant to Securities Regulation?*, 60 U. TORONTO L.J. 941, 943 (2010).

202. *The Market in Initial Coin Offerings Risks Becoming a Bubble*, THE ECONOMIST (Apr. 27, 2017), https://www.economist.com/finance-and-economics/2017/04/27/the-

misinformed investments can easily develop into a widespread panic and a paralyzing uncertainty.[203] When a signal conveys new information suggesting that an investor has dramatically underappreciated the nature or magnitude of a risk to which the investor is exposed, that revelation introduces the possibility that the investor may also be exposed to other underappreciated risks, making previously assumed information insensitivity suddenly sensitive, and causing a change in the investor's attitude across the portfolio.[204] Overall, there are reasons for concern, and the SEC has the necessary legal authority to act as a financial stability regulator, according to § 2 of the Securities Exchange Act, as well as in discharging its investor protection mandate.[205]

IV. POLICY IMPLICATIONS

This Section addresses the policy implications of the preceding analysis to the question of securities regulation of blockchain-based assets. Aiming to clarify the distinction between securities and non-securities offerings on the blockchain, it reviews and criticizes the major legal test applied for when an investment contract is considered a security as articulated by the Supreme Court in *Howey*[206] and recently applied to the blockchain territory by the SEC in the DAO report.[207] It then proposes an initial distinction between two principal groups of investors: sophisticated investors and retail investors. For sophisticated investors, this Article examines the case for a quasi-144(a) private market on the blockchain, allowing trading without registration among sophisticated investors. For retail investors, or in cases of diverse investor profiles, this Article contends that the regulators should assess the embedded costs and risk factors underlying the particular blockchain offering, balanced against the costs of securities regulation. The analysis is then illustrated on three case studies of

---

market-in-initial-coin-offerings-risks-becoming-a-bubble (comparing the blockchain "craze" to the South Sea bubble in the nineteenth century).

203. *See* Judge, *supra* note 164, at 663 (describing the lessons learned from the 2007–2009 financial crisis).

204. *See, e.g.*, *id.* at 699–700 (discussing the investors in the 2007–2009 financial crisis).

205. Hillary J. Allen, *Financial Stability Regulation as Indirect Investor/Consumer Protection Regulation: Implications for Regulatory Mandates and Structure*, 90 TUL. L. REV. 1113, 1126–27 (2016).

206. *See* 328 U.S. 293, 301 (1946) (rejecting the Court of Appeals' test that analyzed whether an investment contract was missing).

207. *See infra* notes 225–238 and accompanying text (describing the DAO case and its implications to blockchain technology).

blockchain-based offerings: Bitcoin, Tezos, and Filecoin. Finally, this Section surveys alternative regulatory baskets that may apply to the blockchain territory, whether as supplemental legal instruments or as alternative regulatory arrangements. Examples of alternative regulatory baskets are: private placements, crowdfunding laws, contracts and consumer protection, financial and money services laws, and state laws.

A. Are Blockchain-based Assets Securities under U.S. Law?

1. The Howey *test*

The question of whether securities regulation applies has to do with whether the offer is designated as an offer of a security.[208] Under § 2(a)(1) of the Securities Act and § 3(a)(10) of the Exchange Act, a security includes "an investment contract."[209] An investment contract is 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.[210] If the offer is categorized as a security (including an investment contract), securities laws and regulations apply, mandatory disclosure is required, public information is provided through EDGAR, and multiple corporate governance implications apply, significantly limiting the contractual freedom of the firm's leadership.[211] If, however, the offer is considered a product or a service, rather than an investment, freedom of commercial speech applies to information disclosed by the corporation to the public, and freedom of contracts applies to the organizational incentives of the offeror. The implications of designating a blockchain and/or its tokens as securities are therefore profound.

The test of whether an offering constitutes a security was established by the Supreme Court in *Howey*.[212] In this case, the respondent offered "units of a citrus grove development coupled with a contract for cultivating, marketing and remitting net proceeds to the investor."[213] Each purchaser was offered both a land sales contract and a service contract, after being told that it "was not feasible to invest in the grove" unless a service contract

---

208. *See, e.g.*, *Howey*, 328 U.S. at 294, 298 (analyzing whether an offering of citrus grove units were securities within the meaning of the Securities Act of 1933).

209. 15 U.S.C. §§ 77(b)–(c) (2012) (defining a security).

210. *See* United Hous. Found., Inc. v. Forman, 421 U.S. 837, 852 (1975) (analyzing the meaning of an investment contract).

211. COX ET AL., *supra* note 8, at 29–30.

212. *Howey*, 328 U.S. at 301.

213. *Id.* at 294.

was made.[214] The land sale contract provided a "uniform purchase price per acre or fraction thereof, varying in amount only with the number of years the plot had been planted with citrus trees."[215] The service contract gave the possession over the land to a party affiliated to the seller, where the company was accountable only for an allocation of the net profits based on a check made at the time of picking. Purchasers in the *Howey* case were, for the most part, non-residents of Florida, predominantly business people who lacked the knowledge and equipment to cultivate citrus groves.[216] The SEC claimed that the transaction constituted an "investment contract" subject to the Securities Act to obligate the seller to uphold the disclosure requirements.[217]

The Supreme Court test for a security is based on both the purchasers' motivation, and on the dependency of the contractual enterprise's success on the efforts of the respondents.[218] In the opinion of the Supreme Court, the purchasers were "attracted solely" by the prospect of a return on their investment, and the cultivation of citrus groves was "seldom . . . economically feasible."[219] It is therefore the dependency on the efforts of the respondents that made the contractual agreement "[a] common enterprise managed by [the] respondents."[220] Even though the rights to the land were legally transferred, the Supreme Court considered the transfer "purely incidental" to the core elements of the transaction.[221] Regardless of the legal terminology, respondents managed, controlled and operated the enterprise, and since the elements of a profit-seeking business venture were present, securities laws were therefore applicable.

Purchaser motivation has served as a test for the securities nature of the offering in cases since then as well. In *United Housing Foundation, Inc. v. Forman*,[222] a housing cooperative in New York City offered apartments through shares of stock that were explicitly tied to the apartment, and the respondent claimed that the Information Bulletin

---

214. *Id.* at 295.
215. *Id.*
216. *Id.* at 296–97.
217. *Id.* at 297.
218. *See id.* at 301. *See generally id.* at 298–99 ("[A]n investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party . . . .").
219. *Id.* at 300.
220. *Id.*
221. *Id.*
222. 421 U.S. 837 (1975).

that accompanied the transaction failed to disclose several critical facts. The test applied by the Court of Appeals was the expectations of profits.[223] The court denied the claim for mandatory disclosure of material facts because the purchasers were attracted solely by the prospect of acquiring a place to live and not by the financial returns of their investment, and hence could not benefit from the protection granted by securities laws.[224]

2. The DAO: SEC report of investigation

In July 2017, the SEC's Division of Enforcement released a report of investigation regarding the question of whether the DAO, an unincorporated organization created by Slock.it UG (Slock.it), a German corporation, and its co-founders and intermediaries may have violated U.S. federal securities laws.[225] In this case, the SEC determined not to pursue an enforcement action, but it did publish a valuable opinion about securities regulation on the blockchain.[226]

The DAO was a "'virtual' organization embodied in computer code and executed on a distributed ledger or blockchain," created by Slock.it and its co-founders in order to "create and hold a corpus of assets through the sale of DAO tokens to investors" for the purpose of making profits.[227] Based on the application of the *Howey* test and as detailed below, the SEC determined in July 2017 that the DAO tokens were securities under the Securities Act of 1933 and the Securities Exchange Act of 1934.[228]

In the spring of 2016, the DAO offered and sold 1.15 billion DAO tokens in exchange for a total of approximately 12 million ETH.[229] Holders of the DAO tokens were granted certain ownership and voting rights in choosing a portfolio of investments to be held by the DAO, via funded projects, which would serve as the underlying asset of the DAO tokens and would grant its owners a return on their investment, respectively.[230] For a project to be included under the DAO's portfolio, a "contractor" needs to submit a proposal embedded in a smart

223. *Id.* at 846.
224. *Id.* at 853.
225. Report on Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 1 (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf [hereinafter Report on Investigation].
226. *Id.* at 1.
227. *Id.*
228. *Id.* at 11 (applying the reasonable expectation of profits test).
229. *Id.* at 2–3.
230. *Id.* at 1.

contract deployed on the blockchain and post details about the proposal on the DAO website, providing a link to the source code.[231] The prerequisites for submitting a proposal were ownership of at least one DAO token and a secured deposit to be forfeited in case the proposal failed to achieve a quorum of DAO token holders.[232] Additionally, before a proposal would be brought to a vote, a group of individuals appointed by Slock.it as "curators" have to review and approve it. These appointed curators had the ultimate control as to whether a project would be submitted for voting by DAO holders. The first proposal to be funded was submitted by DAO's co-founders, Slock.it.

In applying the *Howey* test to the DAO case, the SEC determined the following:

(1) The term "issuer" is broadly defined to include unincorporated organizations or persons, ruling that the term issuer is to be "flexibly construed" in the context of § 5 as the "definition of a security itself expands."[233]

(2) Cryptocurrency is "money" for the purpose of the *Howey* test. Exchanging DAO tokens for ETH is the "type of contribution of value that can create an investment contract under *Howey*."[234]

(3) The motivation of DAO purchasers was to make profits, as the DAO was a for-profit entity, pooling ETH to fund projects, proposing the sharing of profits from the returns of the funded projects.[235]

(4) The efforts of Slock.it's co-founders and the DAO's curators were essential to the success of the DAO's enterprise. The SEC report explains that the "creators of the DAO held themselves out to investors as experts in Ethereum, the blockchain protocol on which the DAO operated, and told investors that they had selected persons to serve as [c]urators based on their experience and credentials." The first proposal was put forth by Slock.it itself.[236]

The SEC stressed that Slock.it's managerial efforts played a significant role in the DAO's success both during the offering and after

---

231. *Id.* at 6–7.

232. *See id.* at 7. ETH raised by the DAO was to be distributed to a contractor to fund a proposal subject to a majority vote of DAO token holders. However, in order to vote, DAO token holders had to tie up their tokens until the end of the voting cycle. As a result, holders were incentivized to either to affirm the proposal in their votes or to abstain from voting. *Id.*

233. *Id.* at 15.

234. *Id.* at 11.

235. *Id.* at 11–12.

236. *Id.* at 12.

the enterprise launched, on an ongoing basis. During the offering, the DAO's protocols were "pre-determined by Slock.it and its co-founders," specifying the powers to be granted to the curators.[237] On an ongoing basis following the launch, the expertise of the curators and their identity "was critical in monitoring the operation of the DAO, safeguarding investor funds, and determining whether proposed contracts should be put for a vote."[238] Although DAO token holders were afforded voting rights, the curators dictated the terms and controlled the scheme of the vote, both by electing the projects that would be brought to the vote, and because DAO token holders had the incentive to either affirm the proposal or abstain from voting due to the technical set-up of the voting process.[239]

The DAO did not meet the requirements of Regulation Crowdfunding, adopted under TIII of the Jumpstart Our Business Startups (JOBS) Act of 2012 because it was not a broker-dealer or a funding portal registered with the SEC and the Financial Industry Regulatory Authority (FINRA).[240]

B. The Case for Antifraud-Only Markets on the Blockchain

One major justification for securities regulation comes from the need to protect the vulnerability of retail investors.[241] However, if we assume that the blockchain offering would be subject to verification of the investor's sophistication, will the market of blockchain offerings effectively reward or penalize voluntary disclosure or its lack thereof? Will other sufficient market mechanisms such as exchanges or other private bodies assume this role? These are somewhat empirical questions to be addressed in future research, documenting the virtual setting of actual blockchain offerings. If the market is exclusively open to sophisticated investors, it is likely that blockchain offerings will be fairly priced given their voluntary disclosures and make investors potentially better off compared to the regulatory universe of mandatory disclosures. For offerings limited to sophisticated investors of securities regimes, an anti-fraud only market providing liquidity similar to the 144(a) market resonates well with the nature of the blockchain.

---

237. *Id.* at 13.
238. *Id.* at 12–13.
239. *Id.* at 13.
240. *See* Report on Investigation, *supra* note 225, at 4 n.11.
241. *See* Langevoort, *supra* note 15, at 1033.

The purpose of Rule 144(a) is to provide a market for the sale of privately placed securities that do not have and are not required to have an SEC registration in place.[242] Mandatory disclosure is generally not required of corporations traded on the 144(a) private market, with the exception of minimal identification such as company name and the nature of its business.[243] Within the 144(a) market, disclosure costs are expected to be reduced, to some extent, and issuers are free of corporate governance implications of securities laws, such as the Sarbanes-Oxley requirements.[244] Remarkably, the 144(a) experience has shown that sophisticated investors demand disclosure approximately the same as required by the SEC in the public market.[245] The 144(a) market is thus a safe haven providing issuers and investors with an unregulated trading platform, exempt from registration and are only subject to anti-fraud rules.[246] Within this private market, the regulatory scrutiny of the SEC is focused only on fraudulent or dishonest manipulation, although the limited scope of action does not necessarily imply a limited enforcement policy. To the contrary, some evidence suggests that the SEC has initiated more fraud investigations against issues exempt from federal registration requirements than against those that were registered.[247]

Parallel with the public market discussed below for investors of diverse profiles, a private liquid market for sophisticated investors will allow better flow of capital to finance innovation and entrepreneurship without jeopardizing the protection of retail investors, while allowing sophisticated investors to negotiate the information they need to assess the offering and to monitor their investment's performance on an ongoing basis. Such a private market will provide blockchain issuers with a choice of regulatory regimes, i.e., a market of informational regulatory regimes. Setting multiple choices for blockchain offerings provides a mechanism superior to a single regulator for ascertaining

---

242. *See, e.g.*, Luis F. Moreno Treviño, *Access to U.S. Capital Markets for Foreign Issuers: Rule 144A Private Placements*, 16 HOUS. J. INT'L L. 159, 174 (1993) (examining the primary purpose behind adopting Rule 144(a)).

243. *See* Sjostrom, *supra* note 14, at 435.

244. *See id.* at 436–37.

245. *See* Treviño, *supra* note 242, at 195 (contending that documentation under Rule 144(a) is becoming a "standardized" practice); *see also* Howell E. Jackson & Eric F. Pan, *Regulatory Competition in International Securities Markets: Evidence from Europe in 1999—Part I*, 56 BUS. LAW. 653, 667 (2001).

246. *See* Sjostrom, *supra* note 14, at 422–23.

247. Joel Seligman, *The Historical Need for a Mandatory Corporate Disclosure System*, 9 J. CORP. L. 1, 34–35 (1983).

what information disclosure is in the investors' best interests.[248] A priori, there is no reason to assume sophisticated investors are less proficient than the SEC in setting the agenda for disclosure requirements. A private market alongside the publicly regulated one will thus provide both blockchain issuers and sophisticated investors with choices, while also revealing investor preferences and thereby providing feedback to regulators on the efficacy of the regulated market, and the nature and type of information that should be subject to mandatory disclosure.

To assess whether sophisticated investors can be assumed to voice their requirements and have sufficient resources to fend for themselves, recall the nature of the embedded costs and risk factors on the blockchain, identified above. Controlling costs and monitoring costs on the blockchain are generally on par with embedded costs and risk factors of traditional investment contracts available in 144(a) private markets, i.e., the traditional core risks encountered by investors in every corporation. Even the sources of systemic risks identified on blockchain-based assets due to impaired transparency and contractual rigidity or "stickiness" are prevalent in MBSs and CDOs, and are not phenomena exclusive to the blockchain.[249] If sophisticated investors can be assumed to demand the information required to assess the investment and to monitor its performance on an ongoing basis in traditional 144(a) markets, then they should also have the requisite decision making skills to fend for themselves when investing in blockchain-based assets, whether personally or by delegating the task to their representatives and advisors.

The standard of eligibility required to deem an investor as sophisticated is also a subject of debate.[250] Currently, the 144(a) market is open only to qualified institutional buyers.[251] Professor Donald Langevoort suggests a thought experiment about why the eligible investor criterion should not be altered to "comfortably include high net worth individuals."[252] Extending Langevoort's

248. Romano, *supra* note 15, at 393.

249. Judge, *supra* note 164, at 690.

250. *See* Fletcher, *supra* note 14, at 1083–84 (discussing different courts' interpretations of what makes an investor sophisticated).

251. *See* 17 C.F.R. § 230.144A (2013). As defined in the Securities and Exchange Commission's (SEC) Rule 501 of Regulation D, a qualified institutional buyer (QIB) owns and invests a minimum of $100 million in securities on a discretionary basis. QIBs typically include savings and loans associations and banks, investment and insurance companies, employee benefit plans, and hedge funds. *Id.*

252. Langevoort, *supra* note 15, at 1060.

thought experiment, why not limit the anti-fraud only standard on blockchain offerings to accredited investors only? Relaxing the requirements of sophistication may resonate well with the libertarian terrain of the blockchain, a market that is typically governed by individual property owners rather than institutions.[253]

Langevoort mentions two more political hurdles for the development of a private anti-fraud only liquid market.[254] The first is the expected political opposition for the private market by agents enjoying the benefits of regulation. The SEC is likely to favor expansion of its regulatory reach for reasons of "regulatory aggrandizement," and the "politically powerful public stock exchanges" are not expected to favor the growth of private rivals into which large sums of money may migrate.[255] The second hurdle is the implicit political motivation to police private power by means of securities regulation. Along with the desire to protect investors, securities regulation "relates to the desire to impose norms that we associate with public governmental responsibility—accountability, transparency, openness, and deliberation" to corporate power.[256] This "administrative law-like" approach to securities regulation is a key toolset for public governance of private power in the traditional economy.[257] The justification for such administrative governance through securities regulation is particularly salient for large corporations and for corporations providing essential services, in particular to systemically important financial institutions (SIFIs) and to socially important non-financial institutions (SINFIs).[258] For these reasons, Langevoort concludes his thought experiment reasoning that the SEC will eventually expand its regulatory authority to the private marketplace as well.[259]

Crypto markets pose unique political constraints. First, a blockchain-based asset is a digital asset positioned on a virtual space and is thus inherently global. Any effort to regulate transactions occurring on the

253. *See infra* note 312 and accompanying text (defining accredited investors); *see also* Langevoort, *supra* note 15, at 1058 (criticizing the net worth standard requirement and its lack of inflation update).

254. Langevoort, *supra* note 15, at 1059 ("First, securities sold pursuant to Rule 144A cannot be fungible with securities traded in a public market. Second, only qualified institutional buyers . . . are currently eligible to participate as buyers.").

255. *Id.* at 1066, 1069.

256. *Id.* at 1066.

257. *See id.* at 1066–67.

258. *See generally* Shlomit Azgad-Tromer, *Too Important to Fail: Bankruptcy Versus Bailout of Socially Important Non-financial Institutions*, 7 HARV. BUS. L. REV. 159 (2017).

259. Langevoort, *supra* note 15, at 1069–70.

blockchain raises questions of extraterritorial jurisdiction.[260] Among other legal difficulties, "the SEC may not be able to effectively pursue bad actors or recover funds."[261] Second, as of early 2018, the type of business financed on the blockchain platforms is typically entrepreneurial, with little political comparability with traditional public sources of power.[262] Third, the blockchain territory is politically positioned as a libertarian safe haven detached from national governments and their administrative agencies.[263] At their core, blockchain-based assets are providing a financial platform based on computation power and mathematical proof, displacing traditional reliance on states, regulators, exchanges, and intermediaries. As of early 2018, the market caps of crypto markets are perhaps not high enough to pose a threat to traditional capital markets, and the intermediaries that serve them. Yet, given the astounding growth rate in crypto markets during 2016 and 2017, traditional regulatory agencies and intermediaries should be concerned, and accordingly, have political motivation to encourage regulation of the blockchain industry.

The political relationship between the regulatory apparatus of the SEC and the blockchain territory encompasses some of the most fundamental questions in international law and policy and in political theory. These questions deal with the intersection between anarchy and capitalism, globalization and the state, free markets and regulation, all of which are beyond the scope of this paper. For our purpose here, it is sufficient to note that trading on the blockchain and traditional 144(a) markets is to a large extent comparable, and the properties of trading on the blockchain by sophisticated investors merit similar protection by securities regulators in applying their authority.

C. Proposed Doctrinal Improvements

As explained above, the *Howey* test for determining whether an investment is protected under securities laws is based both on the

---

260. *See* Anthony J. Colangelo, *What Is Extraterritorial Jurisdiction?*, 99 CORNELL L. REV. 1303, 1319–20 (2014) (noting that Congress cannot independently create cross-border regulatory schemes because it would be an assertion of power beyond the United States's territorial borders).

261. Clayton, *supra* note 6.

262. *See* Cohney et al., *supra* note 96, at 5–6 (conducting an ICO survey and finding that ICOs are primarily used for entrepreneurial business).

263. Adam Winfield, *Blockchain: Libertarian, Authoritarian, or Somewhere In Between?*, FORBES (July 7, 2017), https://www.forbes.com/sites/sap/2017/07/07/blockchain-libertarian-authoritarian-or-somewhere-in-between.

purchasers' motivation to earn profits, rather than consume products or services, and on the dependency of the success of the contractual enterprise on the efforts of others.[264] Blockchain-based assets call into question the rationality of this doctrine.

The first element of the *Howey* test, the motivational element, has given rise to numerous contractual designs of "utility tokens," a term describing blockchain-based assets representing consumptive goods, for the purpose of avoiding securities regulation.[265] In the blockchain territory, discerning consumptive from speculative aspirations is an inherently impractical, vague, and redundant mission. First, all purchasers of blockchain-based assets have a profit-oriented motivation, without reservation. Even when the underlying value of the blockchain-based asset is a consumptive good, there is often a secondary market for tokens.[266] Second, as the analysis of risk factors above shows, blockchain-based assets with consumptive value are often offered to investors in early development stages and incur significantly higher monitoring costs. Purchasers of a blockchain-based asset with a consumptive motivation are often more vulnerable than purchasers with speculative profit motivations. Third, issuers are not well-positioned to assess the purchasers' motivation in the automated trading environment of the blockchain. Issuers rarely meet their investors in person and have little knowledge of their purchase motivation. Requiring offerors of blockchain-based assets to conduct a motivational assessment of their purchasers will inevitably trigger a high degree of uncertainty over the blockchain industry.

The second element of the *Howey* test is an assessment of whether purchasers relied on the efforts of others for success of the enterprise.[267] Blockchain-based assets again challenge the logic of this test. Investors of blockchain-based assets are never positioned to perform the contract on their own. Inevitably, they must rely on the efforts of others on the blockchain's ecosystem to bring their investment to fruition. Yet, when these "others" are dispersed on a decentralized ledger, securities regulation does not make sense, if only for the technically implausible enforcement of mandatory disclosure requirements on a decentralized ledger when no particular party is positioned as the cheaper information gatherer. When purchasers rely

264. *See* SEC v. W. J. Howey Co., 328 U.S. 293, 298–99 (1946).
265. For example, the SAFT project, see Batiz-Benet, *supra* note 9.
266. Hinman, *supra* note 110.
267. *See Howey*, 328 U.S. at 298–99.

on the efforts of a global community of very many others on a decentralized ledger, none of these particular agents are able to carry the costs of mandatory disclosure. Reliance on the efforts of others should be narrowed to test whether a third party—be it a person, entity or coordinated group of actors—drives the expectation of a return or has the potential to exert a controlling cost on the blockchain-based investors.

Regulators should target the identified sources of risks and focus on those risks that securities regulation can potentially mitigate. Securities regulations are particularly useful in taming controlling risks and monitoring risks, and they have some potential value in hedging systemic risks. The potential benefits of applying securities regulations are thus a function of the scope of controlling costs, monitoring costs and potential systemic risks at the particular blockchain offering. The higher the controlling and monitoring costs of the blockchain-based investment contract, the higher the potential need of regulated protection. On the other hand, the costs of regulation must be taken into account and balanced against its benefits.

The costs of securities regulations should also be assessed because regulation is inevitably costly. Application of securities regulations may deter innovation and impede growth, inevitably increasing the costs of funding innovation. Regulators are not technically trained and may make a fortiori poorer decisions about the blockchain's disclosure equilibrium than those achieved by the free blockchain markets. Regulators are themselves agents with self-interested motivations, and thus can be influenced and directed by interest-group politics that may draw on policy that is far from optimal from a societal perspective.[268] Choosing to disclose a certain element might obscure other more important information. Similarly, an adequate warning might be rendered ineffective by inadequate formatting.[269] It is not at all clear what would be the causal relationship between enforcement of securities laws on the blockchain space and blockchain frauds and misbehaviors, and whether enforcement of securities laws on the blockchain offering would enhance the public's welfare given its overall costs.

This proposal is consistent with the *Howey* test's results, albeit contesting its rhetoric. Recall that investors in *Howey* incurred very

---

268. Stephen M. Bainbridge, *Mandatory Disclosure: A Behavioral Analysis*, 68 U. CIN. L. REV. 1023, 1058 (2000).

269. Richard Craswell, *Taking Information Seriously: Misrepresentation and Nondisclosure in Contract Law and Elsewhere*, 92 VA. L. REV. 565, 582 (2006).

high controlling cost, and very high monitoring costs.[270] Investors relied on the management to cultivate the grove for them as they were non-residents of Florida and had no technical expertise in cultivating citrus groves.[271] Yet, in the blockchain setting, the consumption motivation often comes hand in hand with higher monitoring costs, as the consumer value underlying the blockchain-based asset is off-chain and thus cannot be verified automatically.[272] Instead of assessing the purchasers' motivation, offerings of blockchain-based assets require a structural assessment of costs to reveal investor vulnerabilities and assess the regulatory potential to remedy.

D. Examples

1. Bitcoin

In 2008, the pseudonymous Satoshi Nakamoto released a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," which introduced the mechanisms underlying modern blockchains, and in particular the decentralized consensus protocol based on proof-of-work.[273] Shortly afterwards, the same author released open source software implementing these mechanisms, and started running this software themselves on the Internet, thereby creating the Bitcoin blockchain.[274]

In the primary market, Bitcoin has never officially been offered to investors.[275] In the secondary market, its purchase is open to anyone, worldwide, regardless of investor status or qualification, subject to the "proof-of-work" requirement for block-rewards, which essentially allocates the right to assign property rights in the blockchain based on computational power.[276] As of 2018, such computational power is

---

270. *Howey*, 328 U.S. at 296 (noting that the ten-year service contracts generally did not have a cancellation option and gave the service provider "full and complete" possession of the grove).

271. *Id.*

272. For discussion of monitoring costs on blockchain-based assets, see *supra* Section II.B.

273. *See generally* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (unpublished manuscript), https://bitcoin.org/bitcoin.pdf.

274. *See generally Bitcoin*, LUNYR, https://lunyr.com/article/Bitcoin (last visited Oct. 17, 2018) (providing information about Bitcoin's contributors, terminology, history, and structure).

275. *Frequently Asked Questions*, BITCOIN, https://bitcoin.org/en/faq#what-about-bitcoin-and-consumer-protection (last visited Oct. 17, 2018) (explaining that one can only acquire bitcoins (1) as payment for goods or services, (2) by purchasing Bitcoins on an exchanges, (3) a direct transaction with someone near you, or (4) earning bitcoins through mining).

276. *See supra* note 31 (defining proof-of-work).

typically held by Bitcoin miners, who also decide which fork to follow in case of disagreements about the blockchain's rules.[277]

When assessing whether securities regulation should be applied to Bitcoins, controlling costs, monitoring costs, and systemic costs should be weighed against the costs of securities regulation.

First, to assess Bitcoin's possible controlling costs, one should assess whether any particular party is in a position to allocate new blocks or authorize transactions. Bitcoin's blockchain employs a purely automated mathematical process that is open to all, where the power to allocate ownership in new blocks is allocated by computational power to solve mathematical riddles. In 2018, most of this power is held by miners, but their identity and power can shift with time.[278] Indeed, Bitcoin's founder, Satoshi Nakamoto, has not been active on its blockchain since 2010, with no deleterious effect noticed on the blockchain's growth.[279] By contrast, consider the expected effect of the departure of a corporate founder in a traditional corporation to assess the dramatic significance of decentralization. What would happen if Mark Zuckerberg were to leave Facebook? Some efforts to institutionalize the Bitcoin community have evolved throughout the years, but no such community has been granted the power to exert controlling costs on the blockchain. For example, the "Bitcoin Foundation," established in 2012 as a nonprofit, has been funding some of the core software developers of Bitcoin and has represented the cryptocurrency with the U.S. government.[280] "Coin Center," established in 2014, has been advocating Bitcoin to the U.S. government as a think tank.[281] While many parties contribute to the cryptocurrency's growth and share its prophecy and value, no particular entity is positioned to exert controlling costs on the blockchain. Indeed, in June 2018, William Hinman, director of the Division of Corporation Finance at the SEC announced that because Bitcoin has been decentralized and operational for some time, imposing

277. *See* Bloomberg, *This is What the Average Bitcoin Owner Looks Like*, FORTUNE (Jan. 24, 2018), http://fortune.com/2018/01/24/young-men-buying-bitcoin (noting a survey found that nearly half of Bitcoin's investors are minorities and more than 60 percent sit it as an investment).

278. *See generally supra* notes 40–43 and accompanying text (discussing how initially agents with "mining farms" prosper in the process of bidding for new blocks).

279. *See* NARAYANAN ET AL., *supra* note 16, at 171.

280. *Marketing & Operations Plan 2018*, BITCOIN FOUND. (Mar. 30, 2018), https://bitcoinfoundation.org/wp-content/uploads/2018/04/MarkOps-Strategy-2018-V1.1.1-compressed.pdf.

281. *About Us*, COIN CENTER, https://coincenter.org/about (last visited Oct. 17, 2018).

"the disclosure regime of the federal securities laws to the offer and resale of Bitcoin would seem to add little value."[282]

Second, to assess the monitoring costs of the investment contract required in Bitcoin, we must assess whether the value of the token is off-chain or on-chain, meaning whether the blockchain technology offers an automated verification process for the underlying value exchange forming the transaction. In Bitcoin, the value is intrinsic to the token itself and can be verified automatically. The value of the blockchain unit is generally a function of computation processes and transactions occurring *within* the ledger, leading to low monitoring costs.

Third, an assessment of systemic risks is required. The acceleration in Bitcoin value has led many to label it as an asset bubble.[283] But beyond its accelerated value, Bitcoin has limited interconnectivity with other segments of the economy, and as of early 2018, its possible failure is unlikely to pose a threat on the real economy.[284] In December 2017, the economist Jushua Gans posted a postmortem of Bitcoin analyzing the "Bitcoin bubble" "ahead of the game."[285] Gans suggests that Bitcoin has "no fundamentals other than the system itself," and Bitcoin is at risk if "the whole apparatus . . . comes down perhaps from an attack or some other technical failure."[286] Furthermore, a massive sale by a major holder could trigger a market wide panic. Because Bitcoin wallets are technically transparent, the identity of Bitcoin holders is known and can be traced. For example, the Winklevoss twins are well-known for their significant Bitcoin exposure.[287] Yet Gans also points to significant differences from previously known bubbles, which include the global spread of holdings, the digital only trading space, the low trading volumes and the lack of correlation to the real economy.[288] Gans notes that "[u]nlike a stock market or junk bond crash, if bitcoin

---

282. Hinman, *supra* note 110.

283. *See supra* Section III.E.

284. *See, e.g.*, Preeti Varathan, *Most Exonomosts Think Bitcoin Won't Bring Down the Global Economy—Yet*, QUARTZ (Dec. 26, 2017), https://qz.com/1165698/most-economists-think-bitcoin-and-other-cryptocurrencies-arent-dangerous-survey-says (explaining that "most leading European economists believe there's little reason to worry" about the "Bitcoin bubble").

285. Joshua Gans, *The Bitcoin Bubble Post Mortem*, DIGITOPOLY (Dec. 8, 2017), https://digitopoly.org/2017/12/08/the-bitcoin-bubble-post-mortum.

286. *Id.*

287. *See generally* Nathaniel Popper, *How the Winklevoss Twins Found Vindication in a Bitcoin Fortune*, N.Y. TIMES (Dec. 19, 2017), https://www.nytimes.com/2017/12/19/technology/bitcoin-winklevoss-twins.html.

288. Gans, *supra* note 285.

goes down, there are no investments that are curtailed except for the mining operations that underpin the system of course."[289]

To summarize, securities regulation is not an appropriate legal instrument for protecting investors in Bitcoin. Bitcoin has no controlling costs and no monitoring costs, and as of early 2018, it imposes meager systemic risks. On the other hand, attempting to apply securities regulation on Bitcoin would incur heavy costs to the emergence of entrepreneurial platforms and impede innovation that could support economic growth. In addition, securities regulations of Bitcoin would be impractical given the lack of any particular agent positioned as a cheap information provider who could carry the costs of mandatory disclosure. Yet, the *Howey* test would pass Bitcoin as a security with flying colors, as all of its investors aim to profit, and rely on the efforts of others for that process. In Bitcoin, these others are miners on a dispersed platform, exhibiting very low controlling and monitoring costs, suggesting mandatory disclosure afforded by securities laws may not be an appropriate remedy.

2. Tezos

In July 2017, Tezos raised in an ICO 65,627 BTC and 361,122 ETH (worth together $232 million USD at the closure).[290] The ICO was legally designed as a fundraiser, where investors were making non-refundable donations to the Tezos foundation, a corporation seeking (but not yet granted) non-profit status in Switzerland.[291] Tezos's ICO was open to all investor types as a public offering and was promoted in YouTube videos,[292] a Facebook page,[293] and on its website,[294] without discrimination.

Assessing whether securities regulation should be applied to Tezos requires, per the suggested proposal, evaluation of the controlling costs, monitoring costs, and systemic risks of investments in Tezos, to be weighed against the costs of securities regulation of its blockchain. Consider first Tezos's controlling costs. The proceeds of Tezos's ICO

---

289. *Id.*

290. Stan Higgins, *$232 Million: Tezos Blockchain Project Finishes Record-Setting Token Sale*, COINDESK (July 13, 2017, 10:36 AM), https://www.coindesk.com/232-million-tezos-blockchain-record-setting-token-sale.

291. *See generally id.*

292. Tezos, *Tezos, An Explainer Video*, YOUTUBE (May 9, 2017), https://www.youtube.com/watch?v=7m7EU4JWI88.

293. *Tezos Foundation*, FACEBOOK, https://www.facebook.com/tezosledger (last visited Oct. 17, 2018).

294. TEZOS, https://tezos.com/resources (including resources on how to invest).

were collected by the Tezos Foundation, established in Switzerland a few months preceding the ICO in April 2017.[295] According to a "Transparency Memo" posted on Tezos's website, the Tezos Foundation has contracted with Dynamic Ledger Solutions, Inc. (DLS) a U.S.-based company currently controlled by its founders, Kathleen & Arthur Breitman, to purchase "all of the Tezos-related intellectual property (IP), including the source code of the Tezos cryptographic ledger, logos, and trademark applications associated with the name Tezos, domain names, and goodwill arising from a set of a relationships with several contractors and potential customers in the financial technology market" in consideration for payments made to DLS's shareholders, including 8.5 percent of the contributions made during the fundraiser and a ten percent allocation of the tokens in the genesis block, subject the terms of the transaction.[296] In the aftermath of the ICO closure and in light of the class actions filed against the Tezos Foundation and DLS, allegations were made suggesting additional controlling costs collected by DLS shareholders, including requested coverage of legal expenses related to the lawsuits.[297] The disclosure on Tezos's "Transparency Memo" should have sufficed to establish private benefits and a material potential for self-dealing between DLS shareholders and the Tezos blockchain project, based on the position of DLS shareholders as owners of the source code.[298]

Monitoring costs at Tezos are also profound. Per Tezos's "Contribution Terms" posted on its website, investments in Tezos are "non-refundable" and should be considered "contributions" rather than "investments."[299] Remarkably, neither Tezos Foundation nor DLS are contractually obliged to provide purchasers with the tokens. The Contribution Terms explicitly state that the project "could be fully or partially abandoned," and its

---

295. *See generally History*, TEZOS FOUND., https://tezos.foundation/history (last visited Oct. 17, 2018).

296. *Tezos ICO Transparency Memo*, STEEMIT, https://steemit.com/cryptocurrency/@roshania/tezos-ico-transparency-memo (last visited Oct. 17, 2018).

297. Steve Stecklow et al., *Exclusive: Tezos Founders Push for Legal Bailout from Swiss Foundation*, REUTERS (Dec.1, 2017, 6:06 AM), https://www.reuters.com/article/us-bitcoin-tezos-lawsuits-exclusive/exclusive-tezos-founders-push-for-legal-bailout-from-swiss-foundation-idUSKBN1DV4K0.

298. Anna Irrera et al., *Special Report: Backroom Battle Imperils $230 Million Cryptocurrency Venture*, REUTERS (Oct. 18, 2017, 6:06 PM), https://www.reuters.com/article/us-bitcoin-funding-tezos-specialreport/special-report-backroom-battle-imperils-230-million-cryptocurrency-venture-idUSKBN1CN35K.

299. *Contribution Terms*, TEZOS, http://www.tezos.ch/pages/contribution-terms.html (on file with American University Law Review).

network and tokens not developed.[300] No mechanisms for external audit or milestones for monitoring the development of the network were specified in the contribution documents, and indeed, according to the media, Tezos has used the proceeds of its ICO to invest in stocks, bonds, and precious metals, not to hire engineers and code developers, an unusual pattern for a startup company.[301]

Systemic risks are hard to quantify. Investments in Tezos were likely made by investors who had limited ability to trace the sources underlying their investment and potentially producing its cash flow. Investments in such an elusive setting conducted in the enthusiastic market of blockchain issuances of 2017 are prone to inflating the asset bubble where prices skew regardless of fundamentals. The non-refundable nature of the transaction adds to the "stickiness" when no contractual alterations are technically possible.

To summarize, securities regulation is an appropriate legal instrument for Tezos. The public offering incurs significant controlling costs and monitoring costs, and imposes a substantial systemic risk. The purpose of securities regulation is well suited to the case of Tezos and mandatory disclosure is an adequate instrument to mitigate the controlling and monitoring costs of the offering.

3. Filecoin

Filecoin is a blockchain data storage network that has completed its ICO, raising more than $257 million in September 2017.[302] As with Bitcoin, Filecoin miners compete to mine blocks. Yet in Filecoin, tokens represent actual data storage space. Miners compete not only to allocate tokens in the new block per se, but "to amass as much storage as they can, and rent it out to clients."[303] Filecoin mining power is proportional to active storage space on a cloud, which directly provides a useful service to clients.[304]

---

300. *Id.*

301. Oscar Williams-Grut, *What Does a Tech Startup do After Raising $232 Million Selling Digital Coins to Investors? Set up a VC Fund*, BUS. INSIDER (Aug. 13, 2017, 3:05 AM), http://www.businessinsider.com/tezos-launching-vc-fund-investing-stocks-bonds-ico-2017-8.

302. *Filecoin*, COINLIST, https://coinlist.co/filecoin (last visited Oct. 17, 2018) (noting that most of the proceeds were in cryptocurrencies such as Bitcoin and Ether).

303. FILECOIN WHITEPAPER, FILECOIN: A DECENTRALIZED STORAGE NETWORK 1 (July 19, 2017), https://filecoin.io/filecoin.pdf.

304. *See generally*, *Filecoin: A Decentralized Storage Network*, FILECOIN (July 19, 2017), https://filecoin.io/filecoin.pdf.

Despite the allusion to public offerings with the title "ICO," Filecoin's offering was legally designed as a private placement, both in the initial offering stage and on the ongoing trade in secondary markets.[305] The initial offering of Filecoin was exclusively open to accredited investors.[306] Investments in Filecoin had several prerequisites, including creation of a Coinlist account, verification of identity as a US accredited investor, and submission of details required for "Know Your Customer/Anti-Money Laundering" requirements.[307] The ongoing allocation of tokens in the secondary market is decentralized. Miners get paid for fulfilling storage requests on the Filecoin market.[308] As the analysis above shows, exchange platforms exist in traditional 144(a) markets on an anti-fraud only basis, allowing for a liquid market of private securities with reduced regulatory burden for qualified investors.[309] There are strong justifications to extend such regulatory patterns for private blockchain offerings so as to reduce the heavy costs of mandatory disclosure required by securities regulation and to create a market of regulatory alternatives for issuers and investors on the blockchain territory. Per the suggested roadmap, private placements of blockchains should be subject to a quasi-144(a) anti-fraud only requirement. However, to be thorough, this Article will proceed to analyze and assess controlling costs, monitoring costs and systemic risk of the Filecoin offering.

---

305. *See Confidential Private Placement Offering Memorandum: Purchase Rights for Tokens Pursuant to Simple Agreement for Future Tokens*, COINLIST, https://coinlist.co/assets/index/filecoin_index/Protocol%20Labs%20-%20SAFT%20-%20Private%20Placement%20Memorandum-bbd65da01fdc4a15219c49ad20fb9e28681adec9fae744c41cccd124545c4c73.pdf (highlighting the initial requirement that each investor complete a questionnaire proving it is an "accredited investor" for the purposes of the securities laws in order to be eligible to participate in the token sale).

306. *See* FILECOIN, FILECOIN TOKEN SALE ECONOMICS 2, https://coinlist.co/assets/index/filecoin_index/Filecoin-Sale-Economics-e3f703f8cd5f644aecd7ae3860ce932064ce014dd60de115d67ff1e9047ffa8e.pdf (last visited Oct. 17, 2018) ("We are unfortunately legally restricted to involve only accredited investors (world-wide investors accredited to [U.S.] standards or similar . . . .").

307. *How to Invest in Filecoin*, COINLIST https://coinlist.co/assets/index/filecoin_index/How-to-Invest-184a457c99ebf65a45abc72c523ad70e06d3814709d408d93714003128817e64.pdf.

308. Filecoin can be thought of a as a platform for trading in storage space. Filecoin purchasers spend Filecoin hiring miners to store or distribute data. "As with Bitcoin, Filecoin miners compete to mine blocks with sizable rewards, but Filecoin mining power is proportional to active storage, which directly provides a useful service to clients (unlike Bitcoin mining, whose usefulness is limited to maintaining blockchain consensus)." *Filecoin: A Decentralized Storage Network*, *supra* note 304.

309. *See generally supra* Section IV.B.

Analysis of controlling costs, monitoring costs and systemic risks of the Filecoin blockchain offering yields an eclectic pattern. Controlling costs should be separately assessed in the initial offering stage and on an ongoing basis. In the initial offering, distribution of tokens was criticized for an alleged bias giving private benefits to insiders and entrepreneurs.[310] In the secondary market, the decentralized pattern of mining and its storage capacity requirement seem to substantially limit opportunities for tunneling and self-dealing. Monitoring costs are to be tamed in Filecoin by its automated verification process of the underlying value of the blockchain offering.[311] Recall that Filecoin is a centralized storage network in which tokens represent respective storage capacities. Although the underlying value of the token is indeed off-chain, the automated process provided by its code allows for a clear, fast, and accurate verification process of the storage space provided. Filecoin is a good example for saving the costs of monitoring by an intermediary as the storage space it secures is a technical feature that can be automatically verified by the blockchain. Finally, systemic risk should be assessed. The inaccurate pricing is indeed less of a concern when all investors are sophisticated, especially when value of tokens is entrenched in viable storage space granted to token holders.

Notably, applying the *Howey* test on Filecoin would yield a distorted outcome. To be sure, investors of Filecoin had motivation to profit and relied on the efforts of others. But the *Howey* test does not take into account the low monitoring costs afforded by the blockchain's automatic verification process, or the dispersed mining process and its role in sustaining the blockchain-based assets, applying securities laws when they offer little remedy attuned to the identified risks investors face.

E. Alternative Regulatory Baskets

Subsidizing the production of information regarding blockchain-based assets will not necessarily address all the regulatory concerns posed by the changing technological investment environment. Indeed, analysis of the core costs and risk factors detailed above, which could potentially serve to justify additional regulatory instruments, is beyond the scope of this paper. Regulators may address risks

---

310. Stefano Bernardi, *The Analysis Filecoin Doesn't Want You to Read: Digging into the Dynamics of Filecoin's Token Sale and Economy*, TOKENECONOMY (Aug. 4, 2017), https://tokeneconomy.co/the-analysis-filecoin-doesnt-want-you-to-read-e60d5243 f17c.

311. *See generally* FILECOIN WHITEPAPER, *supra* note 303.

stemming from the blockchain with other legal instruments, whether supplementing securities laws or as alternative regulatory baskets.

1. Private placements

Not all security offerings require registration and extensive disclosure. Various exemptions to securities laws apply, where in general, investors of sufficient means are considered sophisticated enough to fend for themselves, whether personally or indirectly with the assistance of advisors and wealth managers. Accredited investors are generally institutions as well as individuals who earn over $200,000 in annual income (or $300,000 jointly, with a spouse) or have a net worth, not including their primary residence, of over $1 million.[312] Originally, securities laws required that the qualification of an investor as accredited would be done prior to any marketing and solicitation efforts, with the burden to verify the investor as accredited on the issuer.[313] However, with the JOBs Act,[314] entrepreneurs can now solicit more aggressively, as well as advertise and post offerings on their websites, without prequalification and as long as they certify the purchaser's accredited status at the back end.[315]

The problem with private offerings is the lack of liquidity in the secondary market. To address this problem, the SEC adopted Rule 144(a), which allows qualified institutional buyers (but not all accredited investors) to trade among themselves and sell freely within the secondary market, as long as the buyer is another qualified institutional investor and is subject only to anti-fraud requirements.[316] The private placement market has grown substantially in recent years. To illustrate, as of 2015, amounts raised through unregistered securities offerings have outpaced

312. 17 C.F.R. § 230.501(a) (2014). This definition has been heavily criticized as it has not been updated with inflation, effectively bringing a wide circle of households into the exemption. Langevoort, *supra* note 15, at 1058.

313. § 230.506(c). Rule 506(c) was mandated by § 201(a) of the JOBS Act. *See* Eliminating the Prohibition against General Solicitation and General Advertising in Rule 506 and Rule 144A Offerings, Exchange Act Release No. 33-9354, https://www.sec.gov/rules/proposed/2012/33-9354.pdf.

314. Jumpstart Our Business Startups Act, Pub. L. No. 112-106, 126 Stat. 306 (2012).

315. DONALD C. LANGEVOORT, SELLING HOPE, SELLING RISK: CORPORATIONS, WALL STREET, AND THE DILEMMAS OF INVESTOR PROTECTION 122–23, 125–27 (2016).

316. Sjostrom, *supra* note 14, at 422.

the level of capital formation through registered securities offerings, and totaled more than $2 trillion during 2014 alone.[317]

2. Crowdfunding

Entrepreneurs can also raise capital from retail investors who do not qualify as accredited investors by way of crowdfunding.[318] Historically, with striking similarity to ICOs offering "utility tokens," crowdfunding was popularized by web platforms such as Kickstarter as a means to bypass the securities laws with returns distributed to investors in assets or other rewards, such as free T-shirts.[319] Utilizing the distinction between consumers and investors based on purchaser motivation allows the issuer to bypass securities laws, as consumers are merely protected per their contractual rights, while investors enjoy extensive protection of securities laws and the SEC. Crowdfunding was justified as an exemption to the securities laws based on the potential protection offered by the "'wisdom' of the crowd," as crowdfunding platforms allow for open discussion between issuers and investors, a deliberative process of communication which is considered a substitute to regulatory monitoring.[320]

Yet, while raising capital on the blockchain is legally ambiguous and subject to regulatory uncertainty and is somewhat of a "no-mans' land," raising capital in crowdfunding is subject to particular legal restrictions. First, crowdfunding laws limit the amount that may be raised. Crowdfunding is limited to a maximum aggregate amount of $1,070,000 in a twelve month period.[321] Second, crowdfunding laws set limits on how much an investor could risk, based on income and net worth (in general, no more than $2200 USD or 5 percent of income or net worth,

317. Scott Bauguess et al., *Capital Raising in the U.S.: An Analysis of the Market for Unregistered Securities Offerings, 2009–2014* (Oct. 29, 2015), https://www.sec.gov/dera/staff-papers/white-papers/30oct15_white_unregistered_offering.html.

318. *See, e.g.*, § 227.100.

319. *See, e.g.*, C. Steven Bradford, *Crowdfunding and the Federal Securities Laws*, 2012 COLUM. BUS. L. REV. 1, 16–20 (2012); Joan McLeod Heminway & Sheldon Hoffman, *Proceed at Your Peril: Crowdfunding and the Securities Act of 1933*, 78 TENN. L. REV. 879, 896 (2011); Jason W. Parsont, *Crowdfunding: The Real and the Illusionary Exemption*, 4 HARV. BUS. L. REV. 281, 283 (2014).

320. *See* LANGEVOORT, *supra* note 315, at 127.

321. *See* Inflation Adjustments and Other Technical Amendments Under Titles I and III of the JOBS Act, Exchange Act Release Nos. 33-10332 & 34-80355 (Mar. 31, 2017), https://www.sec.gov/rules/final/2017/33-10332.pdf.

if they are under $107,000 USD).[322] Third, funding portals are bestowed with monitoring obligations including enforcement of disclosure duties of issuers and supervision of investor profile compliance regarding the investor's education and qualifications. Funding portals are subject to a registration requirement and are legally liable for negligent misrepresentations in crowdfunding.[323]

3. Contract and consumer protection

If securities laws do not apply, the default regulatory basket governing offerings of blockchain units is contract and consumer protection. ICOs or other blockchain offerings are currently unregulated as compared to securities and are not required to have transparency in plans, offering memoranda, and "white papers," and are generally subject to freedom of commercial speech. Offerors can choose what they disclose and the medium and method of disclosure.[324] The main doctrinal vehicle is perhaps the unconscionability doctrine,[325] which has been used to police contracts between consumers and corporations based on flawed bargaining procedure and the doctrine of unilateral mistakes.

However, contract law is both doctrinally outdated and institutionally ill-suited to govern transactions on the blockchain. Contractual enforcement and specific performance are not pertinent to the blockchain territory, as all contracts are automatically enforced. Traditional contractual remedies such as money damages, restitution, rescission, and reformation are hardly realistic when the parties to the transaction are global node users with heterogeneous investor profiles, often obscured under anonymous identities using privacy preserving trading platforms. In addition, courts are ill-positioned to regulate the risks of blockchain units. Their ex post intervention is not sufficiently timely nor based on the availability of participating plaintiffs. The facts provided to the court in any single particular case would rarely suffice to

---

322. *Regulation Crowdfunding: A Small Entity Compliance Guide for Issuers*, U.S. SEC. & EXCH. COMM'N (May 13, 2016), https://www.sec.gov/info/smallbus/secg/rccomplianceguide-051316.htm.

323. Securities Act § 4(a)(1) requires that each intermediary in a crowdfunding transaction be registered with the Commission either as a broker-dealer or a funding portal. Broker-dealers register with the SEC on existing Form BD using FINRA's CRD system, whereas funding portals register on new Form Funding Portal through the SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. Funding portals may begin registering with the SEC on new Form Funding Portal beginning on January 29, 2016.

324. *See* ICO, *supra* note 61.

325. *See generally* Clinton A. Stuntebeck, Comment, 19 ME. L. REV. 81, 85 (1967) (explaining the doctrine of unconscionability's place within contract law).

resolve a blockchain litigated case. Norms and industry standards require broader understanding of the unique and almost peculiar dynamics of the crypto markets. In addition, courts usually lack the requisite technical expertise for understanding and assessing the language of blockchain transactions, which is embedded in code. Courts applying common law on a case-by-case basis are thus institutionally incompetent and, compared with regulators or with the legislature, are at an institutional disadvantage to address blockchain transactions.[326]

Some ex ante regulation of blockchain offerings may be provided by the Federal Trade Commission (FTC). Consumer protection and prevention of unfair and deceptive acts and practices are the hallmark of the FTC's mandate,[327] and could potentially be regulated by the FTC. While as of early 2018, no such regulation has been promulgated, the FTC has turned its attention to blockchain technology and its potential consumer protection implications, and has held several discussions and forums on the subject.[328] In the most recent panel held by the FTC in March 2017, panelists concluded "that it is difficult to determine the scope of the consumer protection risks posed by blockchain technology because it is in a very early stage of development."[329] However, blockchain regulation by the FTC could be forthcoming.

4. Financial services and money services laws

The risks posed by blockchain offerings may also be addressed by financial services and money services law, raising questions of jurisdictional authority between federal and state regulators and between different federal agencies relating to transactions on a blockchain. For example, crypto-securities designated as virtual currencies are sometimes subject to regulation by the Department of the Treasury Financial Crimes and Enforcement Network (FinCEN) as money service businesses

326. For similar arguments for the more general case of consumer protection, see generally Craswell, *supra* note 269, at 592–93; Lewis A. Kornhauser, Comment, *Unconscionability in Standard Forms*, 64 CAL. L. REV. 1151, 1151–52 (1976).

327. Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2012).

328. *See FinTech Forum: Artificial Intelligence and Blockchain*, FED. TRADE COMM'N (Mar. 9, 2017, 9:00 AM), https://www.ftc.gov/news-events/events-calendar/2017/03/fintech-forum-blockchain-artificial-intelligence (announcing the DTC's third FinTech Forum).

329. Kari S. Larsen, *Federal Trade Commission Considers the Implications of AI and Blockchain Technologies*, REEDSMITH (Mar. 15, 2017) https://www.reedsmith.com/en/perspectives/2017/03/federal-trade-commission-considers-the-implication.

(MSB).[330] Regulation of MSB is generally designed to protect consumers in financial transactions, and includes anti-laundering provisions, minimum capital requirements and licensing.

FinCEN regulation applies to some blockchain transactions defined as "virtual currencies," a medium of exchange that operates "like a currency in some environments but . . . does not have legal tender status in any jurisdiction," depending on whether they run on a centralized or decentralized platform.[331] MSB and money transmitters include administrators and exchangers of virtual currency and administrators of centralized repositories of virtual currencies.[332] However, a person who creates units of decentralized convertible virtual currency that has no central repository and no single administrator, which "persons may obtain by their own computing or manufacturing effort," is not subject to regulation as a money transmitter.[333]

Recently, the CFTC has asserted jurisdiction over the regulation of virtual currencies as "commodities" under the Commodity Exchange Act.[334] In October 2017, the CFTC released a report determining that virtual tokens may be commodities or derivatives contracts depending on the particular facts and circumstances.[335] In 2018, a New York district court judge granted the CFTC an injunctive relief, ruling that material misrepresentation and misappropriation of customer funds in contracts of sale of virtual currencies is a fraudulent act with commodities in interstate commerce covered under the CFTC's broad anti-fraud authority.[336]

---

330. 31 C.F.R. § 1010.100(ff) (2017) (stating that a money service business is a person doing business in the United States in one of the listed capacities).

331. *Application of FinCEN's Regulations to Persons Administrating, Exchanging, or Using Virtual Currencies*, DEP'T OF TREASURY (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

332. *Id.*

333. *Id.*

334. *See CTFC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets*, CFTC OFF. OF PUB. AFF. (Jan. 4, 2018), https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf; Commodity Exchange Act, 7 U.S.C. § 1(a)(9) (2012) (defining "commodity" as including "all services, rights, and interests . . . in which contracts for future deliver are presently or in the future dealt in").

335. *A CFTC Primer on Virtual Currencies*, LAB CFTC (Oct. 17, 2017), http://www.cftc.gov/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf.

336. *See* CFTC v. McDonnell, 287 F. Supp. 3d 213, 229–30 (E.D.N.Y. 2018).

5. State laws

Crypto securities have also received the attention of state legislators. One prominent example is the State of New York, whose Department of Financial Services (NYDFS) has issued rules and regulations dealing with virtual currencies.[337] In particular, NYDFS BitLicense regulation requires obtaining a license as a condition of any of the following activities involving New York or a New York Resident, including (1) receiving virtual currency, (2) storing or maintaining custody or control of virtual currency, (3) buying or selling virtual currency, (4) performing exchange services as a customer business, or (5) controlling, administrating or issuing virtual currency.[338] As part of its licensing requirements, New York requires periodic disclosure to NYDFS regulators about ownership, finances, and insurance, as well as the maintenance of a financial reserve, a quasi-equity cushion the amount of which is based on various factors.[339]

Other state regulators intervened in token offerings as well. "Texas was the first state to issue an administrative order on cryptocurrency investments."[340] The Texas Securities Commissioner recently issued two Emergency Cease and Desist orders, first, in December 2017, against USI-Tech Limited, a Dubai-based firm selling investments tied to Bitcoin mining, and second, in January 2018, to the blockchain-based financial system startup BitConnect to cancel a token offering soliciting its investors by claiming to deliver a 100 percent annual return or more.[341] The orders cited "sales agents" targeting Texas residents, as well as residents of other states, "through websites, social media, and online marketplaces like craigslist."[342] Other states may naturally follow, potentially reviving the state-based regulatory competition by establishing a market for crypto-investment law.

---

337. N.Y. COMP. CODES R. & REGS. tit. 23, § 200 (2015).

338. *Id.*; *BitLicense Regulatory Framework*, N.Y. DEP'T OF FIN. SERVS., http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm (last visited Oct. 17, 2018).

339. *See generally* N.Y. COMP. CODES R. & REGS. tit. 23 § 200.8 (2015) (capital requirements); *id.* § 200.14 (reports and financial disclosures).

340. *$4 Billion Crypto-Promoter Ordered to Halt Fraudulent Sales*, TEX. ST. SEC. BD. (Jan. 4, 2018), https://www.ssb.texas.gov/news-publications/4-billion-crypto-promoter-ordered-halt-fraudulent-sales.

341. *Id.*

342. *Id.*

CONCLUSION

Blockchain technology has radically changed innovation funding. Regulators, scholars, judges, investors, and industry players have yet to fully understand this emerging technology and how to potentially regulate it. What is clear is that we lack a structural analysis of the blockchain territory and its technical and economic properties, a perquisite for developing a common language for the establishment of blockchain investments laws to govern the emerging crypto-markets. This Article offers the first comprehensive account for such analysis.

This Article addresses the challenges in protecting investors within this new territory through the lens of securities regulation, providing a systematic analysis of the embedded costs and risk factors of blockchain-based assets, showing that crypto-markets differ materially from traditional capital markets and impose unique controlling, monitoring and technological risk factors. The new investor interface on the blockchain is highly heterogeneous, suggesting that legal deconstruction of the blockchain transaction is required in order to assess whether and when securities regulation is required to protect investors of the identified risks.

Regulators should target their resources in blockchain-based assets that impose types of risks that securities regulation can potentially mitigate. Beyond the practical guidance for securities regulation of the blockchain territory, the analysis sheds light on core questions in securities laws, including their purpose, the breadth of their application in different types of markets, and their exclusivity as a regulatory monopoly.