SECURITY TOKENS: COMPLYING WITH SECURITY LAWS AND REGULATIONS PROVIDES MORE THAN TOKEN REWARDS*

Dafan Zhang**

I. INTRODUCTION

Blockchain has been one of the hottest areas in technology in the last few years. According to a KPMG report, global private investment in blockchain and cryptocurrency has grown from $0.2 billion in 2013 to $4.5 billion in 2018.[1] With the meteoric rise of the cryptocurrency prices in late 2017, leading by Bitcoin price rising from around $1,000 to nearly $20,000 in just about a year's time,[2] mainstream investors took notice and fevered enthusiasm followed.[3] Just like any good ole bubble however, cryptocurrency prices crashed just months later and consequently cooled down enthusiasm to reasonable levels.[4] However, despite this setback, blockchain technology remains a potentially transformative technology capable of shaping every facet of our future, especially in the finance sector.[5]

---

* This article examines the fast-growing area of Initial Coin Offerings (ICOs) and Security Token Offerings (STOs) and suggests that complying with federal security laws and regulations imposed on traditional security offerings provides substantial rewards to issuers and investors. Blockchain technology has grown in prominence over the past two years. Cryptocurrencies have grown from the de facto currencies of the Dark Web and online black markets to popular investment vehicles for the masses. While our government agencies, courts, and legislatures are playing catchup, the emerging market sector has been hit by incidents of fraud, hacks, other security incidents and volatility, eroding public trust and threatening the future prospects of a potentially transformative technology. As the SEC slowly expands its efforts to regulate digital assets, we analyze the application of existing security laws and regulations to STOs and potential benefits of establishing a SEC-compliant security token marketplace.

** Assistant Professor of Business and Entrepreneurship, Lincoln University of Pennsylvania. B.S. West Chester University, M.P.A., University of Pennsylvania, J.D., University of Pennsylvania Law School, cyberphilly@gmail.com.

[1] KPMG, THE PULSE OF FINTECH 2018 18 (2018), https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/the-pulse-of-fintech-2018.pdf.

[2] Stan Higgins, *From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited*, COINDESK (December 29, 2017), https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited.

[3] Some analyst predicted that Bitcoin price would rise to $100,000 while another took a more "cautious" approach and predicted a modest $60,000 price target. Arjun Kharpal, *Bitcoin headed to $100,000 in 2018, says analyst who predicted last year's price rise*, CNBC (January 16, 2018), https://www.cnbc.com/2018/01/16/bitcoin-headed-to-100000-in-2018-analyst-who-forecast-2017-price-move.html.

[4] Bitcoin price crashed soon after those rampant predictions, falling below $10,000 in March 2018, reaching a low of $3,194 on December 15, 2018, and is currently hovering around $3,800 at the time of this article. COINDESK, https://www.coindesk.com/price/bitcoin (last visited March 1, 2019).

[5] Joichi Ito, Neha Narula & Robleh Ali, *The Blockchain Will Do to the Financial System What the Internet Did to Media*, HARVARD BUSINESS REVIEW (March 8, 2017); DOUG GALEN, NIKKI BRAND, LYNDSEY BOUCHERLE, ROSE DAVIS, NATALIE DO, BEN EL-BAZ, ISADORA KIMURA, KATE WHARTON & JAY LEE, BLOCKCHAIN FOR SOCIAL IMPACT MOVING BEYOND THE HYPE, STANFORD BUSINESS SCHOOL CENTER FOR SOCIAL INNOVATION (2018).

This Article focuses on the emerging area of issuance of "security tokens," an imperfect description for a unit of value on a blockchain used to represent fractional equity ownership interests of some underlying asset. Security tokens, in essence, function as digital securities recorded on blockchains.[6] These blockchain-based digital securities offer numerous advantages over other forms of securities. Particularly, digitizing traditional assets on blockchain through this process of "tokenization," also known as "minting,"[7] provides liquidity, transparency, and security, while creating new investments and opportunities across many sectors.[8]

II. BRIEF INTRO IN BLOCKCHAIN

Blockchain technology is a computing data structure which is a type of "distributed ledger technology" (DLT).[9] Put simply, it is just another way to store structured information with computing devices.

A. Distributed Ledger Technology

Traditionally, financial information is stored in a document ordered chronologically called a ledger.[10] Each time a relevant transaction occurs, a new entry is appended or added to the ledger after the latest entry containing the previous transaction record. Prior to the personal computing age, ledgers are kept in journals or books, which are physical, centralized collections of transaction records.[11] With the advent of computers, physical ledgers are digitized in a variety of ways: digital journals, spreadsheets, and databases.[12] Regardless of whether the digital ledgers are kept on a personal computing device or over the internet, however, they are simply digital emulations of a traditional physical ledger–still a centralized collection of transaction records, albeit stored digitally.[13] While abled to be shared, digital ledgers still require centralized custody and control. They require a central operator to ensure the accuracy and

---

[6] Id. at 7; *see also* SECURITY TOKENS, COINDESK, https://coinsutra.com/security-tokens/ (last visited March 1, 2019).

[7] *See* WHAT DOES IT MEAN TO TOKENIZE USD? WHAT DOES IT MEAN TO REDEEM USDC? https://support.usdc.circle.com/hc/en-us/articles/360016278791-What-does-it-mean-to-tokenize-USD-What-does-it-mean-to-redeem-USDC- (last visited March 1, 2019).

[8] See GALEN ET AL., BLOCKCHAIN FOR SOCIAL IMPACT, *supra* note [5].

[9] Sarah Underwood, *Blockchain Beyond Bitcoin*, COMMUNICATIONS OF THE ACM, November 2016, Vol. 59, No. 11, at 15; Carla L. Reyes, *Cryptolaw for Distributed Ledger Technologies: A Jurisprudential Framework*, 58 JURIMETRICS J. 283, 283-302 (2018).

[10] Maurice Herlihy, *Blockchains from a Distributed Computing Perspective*, COMMUNICATIONS OF THE ACM, February 2019, Vol. 62, No. 2, at 78.

[11] *Id.*

[12] *See* Nolan Bauerle, *What is the Difference Between a Blockchain and a Database*? COINDESK, https://www.coindesk.com/information/what-is-the-difference-blockchain-and-database (last visited March 1, 2019).

[13] *Id.*

reliability of the ledger and the transaction records they contain.[14] Banks, for example, rely on such central-operator ledgers to keep track of transaction records for their customers. Bank customers in turn must always look to their banks to obtain accurate and reliably transaction records of their accounts.

Distributed Ledger Technology, or DLT, operates quite differently. "Distributed Ledger" means just that–the ledger is distributed to a group of operators instead of being centrally located.[15] A certain advantage is apparent when transactions records are not in the custody and control of a single operator: redundancy. For example, if two operators are in possession of an identical ledger, if one of the two operators become unavailable, the ledger is still accessible from the other operator. Having more than one operator also reduces the likelihood that the ledger can be tampered with, because a bad actor seeking to tamper with stored information or record false information in a distributed ledger must change all the outstanding ledgers to be effective.[16]

Blockchain is a form of data structure used to store information on computers.[17] It is essentially a chain of data "blocks"–each data block contains a set of data following a pre-defined structure, and each subsequent block is "chained" to the previous block by explicitly referring to the previous block by a digital address.[18] Thus, the blockchain data structure is especially suitable to record financial transaction data due to this sequential chained structure: each financial transaction contains data in a pre-defined structure, linked together chronologically.

The blockchain data structure is uniquely suitable to accomplish distributed ledgers. Due to its "chained" behavior, it is inherently difficult to alter information stored in the blockchain.[19] As a part of its design, during normal operations, the only way to add data to the blockchain is to append new information in the form of new data blocks to the end of the chain.[20] Granted, a single operator can still alter a blockchain and the data blocks it contains by simply rebuilding the chain and substitute an altered data block for an original block from the chain.[21] Add in DLT however, blockchain becomes practically unalterable, or "immutable."[22]

---

[14] *Id*.
[15] Herlihy, *supra* note [10], at 80.
[16] Kelvin FK Low & Ernie GS Teo, LAW, INNOVATION AND TECHNOLOGY, Vol. 9, No. 2, at 235 (2017).
[17] *See* Underwood, *supra* note [9], at 15.
[18] *Id*.
[19] *See* Low et al., *supra* note [16], at 254.
[20] See Underwood, at 15.
[21] It's worth to note that this can also be done through the decision of a majority of operators who consents to doing so, as illustrated by the Bitcoin and Ethereum splits or "forks." *See* Low et al., *supra* note [16], at 241; *see also* discussion *infra* note [35].
[22] It is practically unalterable by an individual or minority of operators. And even if a blockchain is altered through a fork, the original blockchain can live on unaltered, such is the case in Bitcoin Cash and Ethereum Classic. *See* Low et al., *supra* note [16], at 254.

Blockchain-based distributed ledger achieves this immutability by "consensus."[23] Consensus, just as it sounds, indicate an agreement among all operators as to the validity of the ledger in question. Since every operator is in possession of a copy of the ledger, a consensus or agreement can be reached by a majority of the operators with possession of a copy of the ledger as to the accuracy of any single outstanding copy of the ledger. Consensus can be reached a number of ways.[24]

To put it in simpler terms, it is practically impossible for a bad actor or a group of bad actors to produce an altered ledger by recreating (altered or original) data blocks on the original blockchain and distributed the altered ledger to every honest operator. It is practically impossible to do so because all the honest operators will continue to add data blocks to the original blockchain while the altered blockchain is being produced. To overcome the action of the honest operators, any bad actor or group of bad actors must control more computing power than of all the honest operators of the blockchain thus becoming the majority therefore able to reach consensus that the altered blockchain is more trust worthy than the original one.[25]

B. Benefits of Blockchain

Blockchain then, theoretically, carry some great promised advantages over traditional financial systems. In the wake of the Great Recession, consumer confidence in the banking system was low, and blockchain technology aspired to be the solution to the ills of traditional banking system.[26] The following are some of the significant advantages offered by blockchain:

Security. Blockchain offers unmatched security because of consensus. In theory, third parties cannot modify any information stored on the blockchain because there is no centralized control. Aside from the security against bad actors, blockchain is also technologically more reliable because they are not subject to data failures and outages as traditional banking systems which rely on centralized storage.

Transparency. Blockchain offers unrivaled transparency as to the data it stores. Public blockchains and their entire ledgers are viewable to anyone.[27] Once implemented, no single actor can change the transparent nature of the blockchain. This level of transparency is not matched by any traditional data storage systems. While a centralized data controller may offer the entire database for public

---

[23] *See* Herlihy, *supra* note [10], at 80.
[24] *Id.*
[25] *See* Low et al., *supra* note [16], at 254.
[26] Satoshi Nakamoto, the creator of Bitcoin, embedded the message "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" in the initial Bitcoin code, referring to the then-ongoing debate by UK to bail out banks for a second time as a result of the financial crisis. *See* Colin Harper, *Ten Years Later, a Reflection on Bitcoin's Genesis and Satoshi's Timing*, BITCOIN MAGAZINE, Jan. 2, 2019, https://bitcoinmagazine.com/articles/ten-years-later-reflection-bitcoins-genesis-and-satoshis-timing/.
[27] Herlihy, *supra* note [10], at 81.

access, it can just as easily rescind the access, entirely at its prerogative. On the other hand, anyone can browse the entire blockchain and perform searches on any data on the blockchain[28]. Such access to information is permanent and impossible to duplicate through a central-operator system.

Trust. Without centralized control, theoretically, there is more trust in the blockchain. Due to the transparency, immutability, and reliability, users should have more trust in the blockchain and the information it contains.[29]

With the above promises, cryptocurrencies, or "crypto" for short, were born out of the demand for new and better financial systems and the above-mentioned qualities.[30] Cryptocurrencies are monetary instruments built on blockchain to take advantage of its immutability. Because transaction records are permanently saved and not changeable in the future, transactions recorded on blockchains are irreversible in nature. Therefore, cryptocurrencies are more reliable and trustworthy payment systems-they reduce the risk of counterparty to a transaction rescinding or retracting payment.[31]

C. Promises Unfulfilled

However, things have not transpired quite as the blockchain pioneers envisioned. While blockchain technology itself has lived up to its technical reputation, the operators and users of blockchains have not. Instead of security, transparency, and trust, the industry has seen anything but security, transparency, and trust. Instead, some operators and users of cryptocurrencies have developed a shadowy industry whose lack of security has been well documented in a series of security breaches.

Perhaps the most infamous incident came in 2014, when Mt. Gox, once the world's largest Bitcoin exchanges at the time, filed for bankruptcy after losing 744,000 bitcoins valued at over half a billion dollars belonging to users of the exchange due to a security breach.[32] Investigations later revealed that Mt. Gox had long operated with "deeply suspicious patterns" including price manipulations, abnormal accounts, and suspicious transactions before the massive security breach which ultimately brought it to its death.[33]

Bitcoin was far from the only cryptocurrency affected by security breaches. In another blockbuster incident in 2016, Ethereum, another popular

---

[28] A copy of the entire blockchain and its data within can be downloaded by any operator for local access.

[29] *See* GALEN ET AL., BLOCKCHAIN FOR SOCIAL IMPACT, *supra* note [5], at 7.

[30] *See* Jesse Leigh Maniff & W. Black Marsh, *Banking on Distributed Ledger Technology: Can It Help Banks Address Financial Inclusion*? FEDERAL RESERVE BANK OF KANSAS CITY, ECONOMIC REVIEW, THIRD QUARTER 2017, at 53.

[31] Low et al., *supra* note [16], at 236-7.

[32] Jhanile T. Smith, *Bitcoin Exchanges in Bankruptcy: The Square Peg in the Round Hole*, AM. BANKR. INST. J., December 2016; Chayka, Kyle, *Everything You Need to Know About the Mt. Gox Bitcoin Debacle*, TIME.COM. March 1, 2014.

[33] Emerging Technology from the arXiv, *Mt. Gox was riddled with price manipulation, data mining reveals*, MIT TECHNOLOGY REVIEW, February 21, 2019.

cryptocurrency, was also rocked by a high-value security breach. A decentralized autonomous organization ("DAO"), a platform which acts as a "virtual venture capital fund," allowed a perpetrator to exploit an error in its software code and siphoned $50 million worth of Ether (the Ethereum cryptocurrency) from the DAO's main account.[34] Left without any recourse to reverse the transactions on the Ethereum blockchain, the Ethereum team made a controversial decision to split, or "hard fork," the Ethereum blockchain into two: the Ethereum Classic which is the blockchain containing the DAO breach transactions and the new Ethereum which does not contain the DAO breach transactions.[35]

Beyond security breaches, the reliability of the industry infrastructure has also been rocked by other blockbuster incidents. In February 2019, news broke that Quadriga, Canada's largest cryptocurrency exchange, has lost $135 million worth of cryptocurrency it held on behalf of its users.[36] It was reported that Quadriga's CEO Gerald Cotten became sick and died while traveling in India.[37] Somehow his tragic death led to the inability for the exchange to recover all the cryptocurrency assets it was holding on behalf of users because Cotton exerted sole control over the entire exchange with over 100,000 users and over $145 million in cryptocurrency holdings by storing access information to all the holdings on his encrypted laptop, without leaving backup access anywhere.[38] It is almost imaginable that such amount of value can be controlled by a single person on a single device without any sort of backup, but such shocking lapse of trust can and does happen because the lack of regulation on cryptocurrency exchanges.

Security and reliability issues are not the only incidents plaguing the blockchain sector. There are frauds and representations as well. Investor demand for blockchain has also created a new way to raise money–Initial Coin Offerings ("ICO").[39] At the time of this article, there have been reportedly over 5,300 ICOs conducted according to one platform which tracks ICOs, and United States leads the way with over 700 ICOs raising a total of over $7.4 billion in startup capital.[40] However, fast and easy money always bring out the worst in some people, and the ICO landscape is no different. A 2018 study reported that over

---

[34] Usha R. Rodrigues, *Law and the Blockchain*, 104 IOWA L. REV. 679, 680, 704 (2019);

[35] *Id*. at 705-706. Blockchain purist have misgivings regarding the hard fork. The decision to hard fork and thus undo the DAO breach illustrates that the immutability of blockchain can be overcome by consensus-rule, perhaps the start of a dangerous slippery slope. *See Down the Rabbit Hole: Ethereum, Immutability, Consensus-Rule, & Forks*, https://medium.com/social-club/down-the-rabbit-hole-ethereum-immutability-consensus-rule-forks-e9fa8faa9e07 (last visited March 1, 2019).

[36] Jessica Murphy, *Quadriga: The cryptocurrency exchange that lost $135m*, BBC NEWS TORONTO, February 17, 2019, https://www.bbc.com/news/world-us-canada-47203706.

[37] *Id*.

[38] Erica Alini, *How Canada allowed Quadriga's CEO to manage $180M from his laptop with no backup*, GLOBAL NEWS, February 12, 2019, https://globalnews.ca/news/4948599/quadriga-canada-crypto-regulations/.

[39] ICOs are "all the rage in startup financing." Michael Mendelson, *From Initial Coin Offerings to Security Tokens: A U.S. Federal Securities Law Analysis*, 22 STAN. TECH. L. REV. 52 (2019).

[40] *See* TOP COUNTRIES AND ICOS, ICOBENCH, https://icobench.com/stats (last visited March 2, 2019).

80% of all ICOs conducted in 2017 were identified as scams.[41] While slightly late to the game, SEC has been slowly stepping up enforcement against fraudulent ICOs.[42] It appears that the problem is so pervasive that SEC even set up a mock ICO website to warn potential investors of the dangers of ICOs.[43]

Over the last few years, the promise of blockchain technology has been abused by bad actors and bad acts, eroding public confidence in the once promising technology. Blockchain and ICOs create an entirely new class of high-return investments which in turn funds innovation at a grander scale than traditional venture capital.[44] Market confidence is essential, and the security and fraud issues must be adequately and meaningfully addressed if blockchain sector is to continue to thrive and drive future funding of innovation.

III. THE CASE FOR CLEARLY DEFINED REGULATION

It is clear that the blockchain sector needs regulation. As evident in market sentiments and press coverages, enthusiasm in blockchains is waning,[45] and the once touted promises may go unfulfilled if things remain unchecked.

In the early days, regulators have largely taken a "hands-off" approach. Many regulators took a similar approach to the regulation of the Internet in its early days, which left innovation largely unchecked except in cases of individual issues.[46]

A. Lack of Clarity

However, this hands-off approach means the regulatory landscape remains unclear. Several agencies have claimed jurisdiction over blockchains, with conflicting interpretations. As clear evidence of a lack of understanding and clarity, regulators couldn't quite state clearly what a blockchain coin or token is or is not.

SEC has claimed jurisdiction over cryptocurrency as early as 2013, arguing that investment in Bitcoins are securities under the Securities Act of

---

[41] CRYPTOASSET MARKET COVERAGE INITIATION: NETWORK CREATION, BLOOMBERG, https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ (last visited March 1, 2019).

[42] *See id*.

[43] THE SEC HAS AN OPPORTUNITY YOU WON'T WANT TO MISS: ACT NOW!, SECURITY AND EXCHANGE COMMISSION, May 16, 2018, https://www.investor.gov/additional-resources/news-alerts/press-releases/sec-has-opportunity-you-won%E2%80%99t-want-miss-act-now.

[44] Marco Dell'Erba, *Initial Coin Offerings: The Response of Regulatory Authorities*, 14 N.Y.U. J.L. & BUS. 1107, 1120 (2018).

[45] Data reportedly shows that as of January 1, 2019, almost 1,000 altcoins, or blockchain coins or tokens other than Bitcoin, has simply became inactive or disappeared. *See* William Suberg, *While Bitcoin 'Died' 90 Times In 2018, There Are Almost 1000 'Dead' Altcoins, Data Shows*, COINTELEGRAPH, January 1, 2019, https://cointelegraph.com/news/while-bitcoin-died-90-times-in-2018-there-are-almost-1000-dead-altcoins-data-shows.

[46] *See* Dell'Erba, *supra* note [44], at 1122.

1934 (the "Securities Act") because they are both investment contracts and notes.[47] In siding with the SEC in *SEC v. Shavers*, the Eastern District of Texas applied a test from *SEC v. W.J. Howey & Co*., 328 U.S. 293, 298–99 (1946) (the "*Howey* Test"), and found that Bitcoins can be used as money; defendant Shaver's promise of returns on investors' investments showed a common enterprise; and there was certainly an expectation of profit derived from the efforts of a third party.[48] Therefore, the court determined that the Bitcoin investments were securities.[49]

Subsequently, SEC has taken the public position that many coins or tokens meet the definition of securities under the Securities Act thus must register with SEC or be exempted from doing so.[50] Further, platforms which offer trading of such digital assets qualifying as securities must also register as a national securities exchange or be exempt from doing so.[51] SEC has also stepped up the pace of enforcement actions taken against ICOs and exchanges subsequently.[52] While earlier enforcement actions has focused more on fraudulent ICOs, SEC nonetheless has recently started enforcing the registration requirements against ICOs and exchanges.[53] However, despite the increased efforts of enforcement, ICOs continue to occur amidst the ambiguous belief that certain tokens are not securities under the Securities Act and the *Howey* Test and are outside the purview of the SEC.[54] The Internet was subsequently flooded with confusion and speculating opinions.[55]

---

[47] The Eastern District of Texas rejected defendant Shaver's argument that Bitcoin is not money and is not regulated by the United States. *Sec. & Exch. Comm'n v. Shavers*, No. 4:13-CV-416, 2013 WL 4028182, at *1 (E.D. Tex. Aug. 6, 2013), adhered to on reconsideration, No. 4:13-CV-416, 2014 WL 12622292 (E.D. Tex. Aug. 26, 2014).

[48] *Shavers*, 2013 WL 4028182, at *2.

[49] *Id*.

[50] Statement on Potentially Unlawful Online Platforms for Trading Digital Assets, SECURITY AND EXCHANGE COMMISSION, March 7, 2018. https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading.

[51] *Id*.

[52] SEC publishes a list containing 30 enforcement actions against digital assets/ICOs spanning from July 2013 to February 2019. While the number of ICOs overwhelmingly dwarf the number of enforcement actions, 18 or the 30 actions were in the year of 2018 alone, suggesting an increase in enforcement focus in the last year. *See* Cyber Enforcement Actions, SECURITY AND EXCHANGE COMMISSION, https://www.sec.gov/spotlight/cybersecurity-enforcement-actions (last visited March 1, 2019).

[53] Starting in September 2018, SEC instituted enforcement actions against unregistered broker-dealer in TokenLot LLC, Lenny Kugel, and Eli Lewitt; unregistered national securities exchange in Zachary Coburn; and unregistered offering of tokens as securities in CarrierEQ, Inc., d/b/a Airfox and Paragon Coin, Inc. *See id*.

[54] SEC's director of Division of Corporation Finance, Willian Hinman, commented in a congressional testimony that it is possible that certain token sales might not constitute the sale of securities if the buyer or holder of the tokens bought the tokens for their utility instead of for investment purposes. *See* Aaron Stanley, *SEC Official Offers New Hope for Utility Tokens in Congressional Testimony*, FORBES, April 28, 2018. https://www.forbes.com/sites/astanley/2018/04/28/sec-official-offers-new-hope-for-utility-tokens-in-congressional-testimony/#2e19ff7dfcf9; *see also*, Michael J Casey, *Regulators Are Slowly Starting to Get It: Utility Tokens Are Real*, COINDESK, https://www.coindesk.com/regulators-are-

The Commodity Futures Trading Commission ("CFTC") has also claimed jurisdiction over cryptocurrencies because it declared "virtual currencies to be a 'commodity' subject to oversight under its authority under the Commodity Exchange Act (CEA)".[56] This jurisdictional claim has been challenged and upheld by the Eastern District of New York.[57] Recently, CFTC issued a Primer on Smart Contracts, introducing self-executing smart contracts to the public while in part reminding the public that smart contracts are subject to existing financial laws including the CEA.[58]

The resulting regulatory landscape is a "multifaceted, multi-regulatory approach."[59] It is a polite way to describe a dysfunctional regulatory landscape. This would not be the first time SEC and CFTC engaged in jurisdictional disputes over a newly emerged financial instrument. Decades ago, SEC and CFTC faced a jurisdictional conflict over modern OTC derivatives.[60] It is similar to the current ambiguity over blockchain: was OTC derivatives securities or futures of commodities? This jurisdictional conflict was partially resolved by the passing of "Treasury Amendment" to the CEA by Congress, exempting certain OTC derivative transactions from the CEA.[61] Further legislative and administrative changes subsequently reduced the jurisdictional overlap.[62] As a result, most OTC derivatives are now classified as securities and are only subject to one regulatory regime under SEC.[63]

The lack of consensus on blockchain cannot continue. Regulatory clarity and clear legal structures are essential for any financial market and is crucial to

---

slowly-starting-to-get-it-utility-tokens-are-real.

[55] *See, e.g. What Are Utility Tokens, And How Will They Be Regulated*? December 28, 2018, https://blog.sfox.com/what-are-utility-tokens-and-how-will-they-be-regulated-89cfb6bb2a45 (speculating how utility tokens will be regulated); compare to this article suggesting that utility tokens should not be "considered or advertised as investments, and therefore avoid falling under government regulations."; s*ee also Security vs. Utility Tokens*, April 27, 2018, https://blog.bankex.org/security-vs-utility-tokens-bc9e71e15544.

[56] CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets, CFTC, January 4, 2018, https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf

[57] "CFTC has standing to exercise its enforcement power over fraud related to virtual currencies sold in interstate commerce." *Commodity Futures Trading Comm'n v. McDonnell*, 287 F. Supp. 3d 213, 230 (E.D.N.Y.), adhered to on denial of reconsideration, 321 F. Supp. 3d 366 (E.D.N.Y. 2018).

[58] A Primer on Smart Contracts, CFTC, November 27, 2018, https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf.

[59] CFTC Backgrounder, *supra* note [57].

[60] J. Christopher Kojima, *Product-Based Solutions to Financial Innovation: The Promise and Danger of Applying the Federal Securities Laws to OTC Derivatives*, 33 AM. BUS. L.J. 259, 305 (1995).

[61] 7 U.S.C. § 2(ii) (1994).

[62] Kojima, *supra* note [61], at 306.

[63] "OTC options on equity securities or on U.S. government securities, for example, are securities within the meaning of Section 3(a)(10) of the Exchange Act." Final Rule: OTC Derivatives Dealers, 17 CFR §§ 200, 240, 249.

the blockchain sector's future.[64] This article calls for greater clarity in understanding the different blockchain implementations and suggests clear definitions for regulatory purposes. In particular, blockchain tokens representing equity interests should be distinguished from cryptocurrencies and be recognized as "securities" thus subject to the jurisdiction and regulation by SEC as securities.

B. Coin vs. Token

Since the early days of blockchains, the terms "coin" and "token" were used interchangeably. Generally, units on a blockchain can be referred as either coins or tokens.[65]

As of late, coins and tokens diverge both in terms of their function and perception. While some blockchain coin or token offerings are still being referred to as ICOs, a new term–Security Token Offerings ("STO")–is emerging.[66] The blockchain is slowly distinguishing cryptocurrencies as coins, and security tokens as functionally distinct and appear to be securities.[67] Therefore, this article proposes officially distinguishing coins and tokens as two distinct species of blockchain implementations. Doing so may help regulators, courts, and other stakeholders clarify how different blockchain implementations should be viewed and treated.[68]

---

[64] For example, Richard Lindsey, SEC Director of Market Regulation, opines that lack of regulatory clarity on TOC derivatives "creates enforceability questions which, in turn, have a destabilizing effect on the global financial markets." Federal Securities Report Letter 1851, FED. SEC. L. REP. P 35991519; also according to the SEC, mortgage investors believe that "vibrancy and effectiveness of the U.S. capital markets depends on the clarity and certainty of legal and regulatory structures." Companies Engaged in the Business of Acquiring Mortgages and Mortgage-Related Instruments (Release No. IC-29778; File No. S7-34-11), 2011 WL 5854541, at *4.

[65] Merriam-Webster dictionary lists "a unit of a cryptocurrency" as one of the definitions for both "coin" and "token"; Ethereum foundation describes Ethereum as "a tradeable digital token that can be used as a currency, a representation of an asset, a virtual share, a proof of membership or anything at all" https://ethereum.org/; *see also*, Roger Aitken, *Crypto Financial Platform OpenLedger Goes 'Wall Street' With New ICO Investments*, FORBES, October 23, 2016, https://www.forbes.com/sites/rogeraitken/2016/10/23/crypto-financial-platform-openledger-goes-wall-street-with-new-ico-investments/#6856cbc22f78 (ICOs allow investors to gain exposure to an asset through a token).

[66] Node Blockchain in a study entitled "*Security Token Offerings The Evolution of Capital Formation*" defines STO as "a financial security issued in the form of a digital asset" representing ownership rights in underlying assets; Commentators distinguish STOs from ICOs because the tokens investors receive are "actual stakes in the business or project and its assets." Aashish Sharma, *Will STOs (security token offerings) rule over ICOs in 2019*? January 12, 2019, https://hackernoon.com/will-stos-security-token-offerings-rule-over-icos-in-2019-8feda7bcf562.

[67] *See* Node Blockchain, *supra* note [66], at 7.

[68] There are expected to be many unanswered legal questions involving security tokens. *See* Reyes, *supra* note [9]. Agreeing on clear definitions and voluntary submission to SEC jurisdiction may help advance blockchain jurisprudence.

First, the term "coins" suggests a monetary instrument.[69] On the other hand, "token" suggests an instrument of value with certain conditions.[70] For example, at an arcade, you will be prompted by video game machines to "insert coins" to play. Depending on the arcade, you may insert actual US currency coins, or tokens which are issued by the arcade to operate the machines. The function and value are similar to the holder relating to the machine: they can both be used to operate the machine. However, the function and value to the holder differ aside from the machine-the distinction is that currency coins can be used to purchase other things elsewhere, while tokens may be strictly restricted to the underlying value to a particular issuer.[71]

Applying the above distinction between the two, this article proposes that blockchain security tokens, or simply tokens, are defined as blockchain-based value units representing an underlying value in its issuer. Thus, tokens function similarly to cryptocurrencies technically, except that they represent different interests or values. Unlike cryptocurrencies which simply represents a value construct which are designed to be unrestricted, the value of tokens is derived from and primarily restricted to underlying interest in its issuer. This definition puts tokens squarely within the definition of securities under the *Howey* Test.
There are then two common types of tokens based on primary function:

Security tokens. Security tokens represent equity stake, or ownership in a company.[72] Virtually any type of asset can be tokenized or digitized on a blockchain so units of fractional ownership can be represented by tokens. Proponents of security tokens agree with the view that security tokens representing interests in underlying assets are securities under the *Howey* Test, thus are subject to the regulation under the Security Act.[73]

Utility tokens. Utility tokens allow holders access to a blockchain-based network so they can utilize the resources or services on the network. They function like gaming tokens used in arcades, which can be exchanged to operate games but holds no actual cash value.[74] Many have argued that utility tokens are

---

[69] Merriam-Webster dictionary provides both "a usually flat piece of metal issued governmental authority as money" and "a unit of a cryptocurrency" among its definitions.
[70] Merriam-Webster dictionary provides "a piece resembling a coin issued for use (as for fare on a bus) by a particular group on specified terms", although it also provides "a unit of a cryptocurrency" as a definition.
[71] "Tokens generally differ from coins in their usefulness. A coin is issued by a government, and can be exchanged freely for any goods, services or other coins. However, a token is generally limited in its use. There is often one specific purpose for a token." MONACO RARE COINS, May 17, 1998, https://www.monacorarecoins.com/local-currency-token-coins/.
[72] S*ee* Node Blockchain, *supra* note [66]; *see also* Sudhir Khatwani, *What Are Security Tokens & Why Is the Market Bullish About It?* COINSUTRA, February 21, 2019, https://coinsutra.com/security-tokens/.
[73] While arguments can be and have been made that certain security tokens may not meet the *Howey* test, this article takes the approach that all security tokens meet the *Howey* test and therefore should comply with applicable federal securities laws. See Noelle Acheson, *Security Tokens vs. Tokenized Securities: It's More Than Semantics*, COINDESK, February 2, 2019, https://www.coindesk.com/security-tokens-vs-tokenized-securities-its-more-than-semantics.
[74] *See supra* note [55].

not securities under the *Howey* test because their primary purpose is not to be held for future profit.[75] Of course, like all things of value, utility tokens defined this way may still find secondary markets where they are traded or exchanged without the involvement of the token's issuer. In that sense, it is not clear whether such investment purpose satisfies the *Howey* Test.[76]

Regulatory clarity can be achieved through presuming all token are securities, then establish clear guidance on how to exempt certain tokens from the securities classification.[77]

C. Alignment with Existing Federal Securities Laws

Under the Securities Act, all security offerings must be registered with the SEC unless they qualify under an exemption.[78] Registration with the SEC involves providing the agency essential facts regarding the security offeror's company.[79] Registration is a complex process with heavy cost burdens to the issuer, and are generally disfavored by companies seeking equity financing in the startup stages.[80]

For companies looking to avoid the registration process, there are several exemptions they might qualify under. Qualifying under one of the exemptions does not mean that securities offerings can be conducted without any involvement with SEC however–securities issuers must still make disclosures to SEC, the requirements are just not as complex as what is required through the registration process. This section will very briefly examine each of the commonly used securities offering exemptions and the respective regulatory requirements posing challenges to security token issuance under each exemption.[81]

---

[75] It could be argued that utility tokens do hold value on the secondary market by speculators and non-speculators alike (the underlying utility may rise in value in the future), it is unclear whether they meet the "primary purpose" prong of the *Howey* test. This article does not focus on utility token and thus does not take a position on utility tokens.

[76] It is conceivable that an issuer may conduct a utility token offering with the sole purpose of creating secondary market investment opportunities.

[77] Such is the regulatory scheme for registering security offerings: all are presumed to be required to register unless otherwise exempted from doing so. *See* 15 U.S.C.A. § 77f; Registration Under the Securities Act of 1933, SEC, https://www.sec.gov/fast-answers/answersregis33htm.html (last visited March 1, 2019).

[78] *See id*.

[79] *See id.*

[80] *See* Merritt B. Fox, Regulating Public Offerings of Truly New Securities: First Principles, 66 DUKE L.J. 673, 677 (2016).

[81] While comparatively simpler than registering a security, the SEC rules and regulations nonetheless sets forth various detailed requirements for each type of securities offerings exempted from registration. This section limits the discussion for certain core technical requirements most relevant to the offering of security tokens. For a thorough examination of the different registration exemptions and their respective requirements, see

Securities and transaction exemptions under federal law, 4 TREATISE ON THE LAW OF CORPORATIONS § 27:15 (3d).

1. Private Placement (Regulation D Rule 506(b))

Under Rule 506(b) of Regulation D, a securities offering is exempted from registration if the offering is conducted (a) without general solicitation; (b) to no more than 35 non-accredited investors; and (c) by offering restricted securities with limited transfer rights.[82] Additionally, an issuer must also (a) require non-accredited investors make financial disclosures similar to those required of accredited investors; (b) provide specific financial statements to the non-accredited investors; and (c) be available to discuss the offering with non-accredited investors.[83]

2. General Solicitation (Regulation D Rule 506(c))

Under Rule 506(c) of Regulation D, a securities offering is exempted from registration even with general solicitation, if the offering is conducted to all accredited investors and the offeror takes reasonable steps to verify purchaser's accredited status.[84]

3. Limited Offering (Regulation D Rule 504)

Under Rule 504 of Regulation D, a securities offering is exempted from registration if it is a limited offering, meaning the offeror must only raise $5 million or less in a given 12-month period, and is not a restricted business type.[85]

4. Crowdfunding (Regulation CF)

Under Regulation CF, a securities offering is exempted from registration if (a) it is conducted online through a SEC registered intermediary such as a broker-dealer or funding portal; (b) the offeror raises a maximum aggregate amount of $1,070,000 in any 12-month period; and (c) individual investors are limited to an aggregate investment amount calculated based on their net worth or annual income across all Regulation CF offerings in any 12-month period.[86]

5. Regulation A

Under Regulation A, which has two tiers: tier 1 and tier 2, a securities offering is exempted from registration if the company is not a prohibited business type and meets certain aggregate offering limits: tier 1 offerings must be limited to $20 million or less over any 12-month period while tier 2 offerings must be

---

[82] 17 C.F.R. § 230.506.
[83] *Id.*
[84] 17 C.F.R. § 230.506(c).
[85] 17 C.F.R. § 230.504.
[86] 17 C.F.R. § 227.100.

limited to $50 million of less over any 12-month period. To qualify for the higher offering limit, an offeror must also place a limit on non-accredited amounts; disclose audited financial statements, and file ongoing reports with SEC.[87]

6. Intrastate Offerings

Under Section 3(a)(11) of the Securities Act, a purely intrastate offering is exempted from registration if (a) the offeror is organized in the state where it is offering securities; (b) the offeror's principal place of business is in the state where it is offering securities; and (c) each purchaser make written representation proving the residency of the purchaser.[88]

For convenience, the essential functional requirements under each of the foregoing exemptions are presented in Table 1.

Table 1

Relevant Functional Requirements of Registration Exemptions

Exemption	**Reg D**			**Reg CF**	**Reg A**		**Intrastate**	
Functional Requirement	**Rule 506(b)**	**Rule 506(c)**	**Rule 504**		**Tier 1**	**Tier 2**	**Rule 147**	**Rule 147A**
General Solicitation	No	Yes	Limited	Registered Intermediary	Yes	Yes	In-state	Yes
Issuer Restrictions			Yes	Yes	Yes	Yes	In-state	In-state
Investor Status Screening	Yes	Yes		Yes		Yes	In-state	In-state
Investment Limits				Yes		Yes		
Rolling Offering Limit			Yes	Yes	Yes	Yes		
Resale Restriction	Yes	Yes	Yes	Yes	Yes		Yes	Yes

[87] 17 C.F.R. § 230.251.
[88] 15 U.S.C.A. § 77c(a)(11); 17 C.F.R. §§ 230.147, 230.147A.

IV. IMPLEMENTATION AND ADAPTATION

A. Functional Requirements

Based on Table 1 and the foregoing discussion, the following are technical requirements necessary to address compliance needs if an issuer wishes to rely on a registration exemption to conduct a STO compliant with securities laws and regulations: (1) Investor Status Screening; (2) Rolling Investment limit; (3) Rolling Offering Limit; and (4) Resale Restriction.[89]

Out of the four functional requirements, only Resale Restriction is capable of self-execution on chain without external input through the use of smart contracts. To implement resale restriction of a security token, a function can be programmed on-chain as a self-executing smart-contract that any security token transfer transaction cannot be completed during a certain time period or under certain conditions. In other words, a transfer of the security token can only be completed if it is outside of a stated time period and meeting a set of defined conditions. Encoding such restrictions can satisfy the Resale Restriction requirement for all the offering exemptions.

On the other hand, all the other functional requirements cannot be easily and satisfactorily accomplished completely on-chain as self-executing smart contracts without external input. It is arguable that both Rolling Investment Limit and the Rolling Offering Limit can be performed on-chain–after all they should only involve mathematical operations which sum up related transaction amounts, either investments by a certain investor or total supply of security tokens, and ensure the resulting sum stay under a certain threshold. However, that would only be sufficient if the particular security token is the only token that the issuer or the investor has access to. To circumvent any amount threshold residing on-chain, the issuer simply has to offer a brand-new token.[90]

The Investor Status Screening is also ill-suited to be performed on-chain. It is conceivable that investor screening can be performed through the use of a smart contract by requiring the proposed purchaser of the token to meet certain pre-defined criteria. However, such automated validation may not meet the "reasonable effort" necessary to verify investor status called for by various offering exemptions.[91]

---

[89] The general solicitation and issuer's business type requirements are directed to the issuer and not the securities being offered, therefore are omitted from discussion here.

[90] In such a case, each individual set of tokens offered could be below the Rolling Offering Limit, but over the Rolling Offering Limit if combined for said multi-token issuer.

[91] The Fifth Circuit has held that a "multi-step procedure" as reasonably investigation: (1) nomination of wealthy investors by bank managers; (2) brokers were questioned about the suitability of their clients; (3) investors were asked to fill out a questionnaire about net worth and financial sophistication; and (4) the questionnaires were reviewed by an executive of the issuer before securities were sold. *Mary S. Krech Tr. v. Lakes Apartments*, 642 F.2d 98, 102 (5th Cir. 1981). Therefore, a single un-supervised and un-audited screening based on investor self-disclosure without an effort by the issuer to investigate may ultimately not be enough.

B. Which Exemptions Should Token Issuers Consider?

Based on the regulatory requirements stated above, a few exemptions appear not to be very suitable for the average token issuers.

First, Intrastate offerings under Rule 147 or Rule 147A are not suited for STOs because of their strict territorial constraints.[92] Blockchain is an Internet technology, by its nature it is interstate.[93] While the technology sector has attempted to apply territorial constraints in other use cases such as online gambling, the success of geospatial limiting technologies is not foolproof.[94] In other words, a self-executing smart contract cannot reliably determine the location of a potential buyer to ensure that they are in-state.

Second, Rule 506(b) exemption does not allow general solicitation, therefore is not well suited for the purpose of STOs. Aside from fundraising, ICOs have served as a marketing tool, generating buzz among the public about the underlying issuers and their products and services. The inability to publicly solicit the offering and market the products and services greatly diminish the usefulness of the offering.

Third, Regulation Crowdfunding must be conducted on an internet platform through a registered intermediary.[95] It is not suitable for self-issuance, but may be suitable through a third party intermediary such as an exchange.[96] However, the 12-month Rolling Offering Limitation of $1,070,000 means that CF offerings may not meet the needs of many issuers which are looking for larger amount of financing. Additionally, at the time this article is written, there are relatively few registered intermediaries which both satisfy Regulation Crowdfunding and offer blockchain services. It is possible that blockchain-based crowdfunding will grow and become a more suitable option for smaller and early-stage issuers in the near future.

C. Functional Approaches for Tokens to be Regulatorily Compliant

Based on the functional requirements under the various offering exemptions, this article discusses two approaches on how security tokens can satisfy the functional requirements of the offering exemptions described above.

---

[92] *See* 15 U.S.C.A. § 77c(a)(11); 17 C.F.R. §§ 230.147, 230.147A.

[93] Multiple courts have held that transmission of material over the Internet constitutes interstate commerce. *See United States v. Lewis*, 554 F.3d 208, 215 (1st Cir. 2009); *United States v. Carroll*, 105 F.3d 740, 742 (1st Cir. 1997); *United States v. MacEwan*, 445 F.3d 237, 244 (3d Cir.2006).

[94] For example, location spoofing, or using technology to pretend that a computer is in a location that it is not physically located in, continues to pose as an increasing challenge to the online gambling industry, where casino licensees are required by law to limit their games only to gamblers physically located in the state it is licensed to operate in. *See* Philip Conneller, *Spoofing is Now the Online Gambling Industry's Biggest Cyber Headache, Per Report*, CASINO.ORG, October 19, 2018, https://www.casino.org/news/spoofing-is-now-the-online-gambling-industrys-biggest-cyber-headache.

[95] 17 C.F.R. § 227.100.

[96] See regulatory compliant exchange discussed *infra*.

Notably, the two approaches differ in where the functional requirements are met: on-chain or off-chain. Although the end goal of each method is the same, where the functional requirements are incorporated into the process lead to practical, theoretical, and philosophical differences in the implementation of blockchain technology. Under the first model, functional requirements are incorporated into the blockchain by embedding technological functions into the tokens, whereas under the second model, blockchain is utilized by incorporating the technology into an existing, established process of offering securities. The next section discusses how both approaches can be implemented by securities issuers.

V. PROPOSED APPROACHES

In view of the above stated regulatory framework, this section examines how security token issuers can stay compliant with securities regulations when they issue security tokens. Fundamentally, this article examines two approaches to attempt to achieve compliance, plus a third proposal which would enhance either of the two approaches.

First, any issuer planning a STO can ensure that the tokens being issued are technically compliant with securities regulations by adhering to a regulatorily compliant Compliance-Capable Token Protocol.

Second, issuers can conduct a traditional non-token securities offering, and offer investors blockchain security tokens as a digital representation of their security interests.

Third, issuers utilizing either the first or second approach can opt-in to a self-regulated exchange where standardized information disclosures are collected, stored, and displayed for the benefit of investors.

A. The Compliance-Capable Token Protocol

Under this first model, functional requirements are incorporated into the blockchain by encoding smart contracts into a Compliance-Capable Security Token which validates the various functional requirements necessary for achieving regulatory compliance.

There are already token standard protocols which exist to standardize and facilitate orderly trading of tokens. For example, on the Ethereum network, ERC-20[97] is a widely accepted standard for minting tokens.[98]

The ERC-20 standard defines a set of mandatory rules which must be incorporated into a token on the Ethereum network. Those rules set forth how tokens are transferred and how data within each token is stored and accessed.[99]

---

[97] ERC stands for Ethereum Request for Comment, and the number 20 was the number assigned to the request for a token technical standard. See ERC: Token standard #20, https://github.com/ethereum/eips/issues/20 (last visited March 1, 2019).

[98] According Etherscan, there are 893 tokens with 172,840 token contracts at the time of writing. TOKEN TRACKER, https://etherscan.io/tokens (last visited March 12, 2019).

[99] *See* CREATE YOUR OWN CRYPTO-CURRENCY WITH ETHEREUM, https://www.ethereum.org/token

Therefore, tokens minted pursuant to the ERC-20 standard can be transferred or accessed using a standard set of procedures, making their transfer more efficient and convenient.

Following the ERC-20 standard, Ethereum developers developed several subsequent standards extending the ERC-20 token by adding additional requirements while preserving those set forth in the ERC-20 standard.[100] One of those newer standards, ERC-1404, was designed to extend ERC-20 by incorporating requirements which, in theory, help with legal and regulatory compliance.[101] In essence, the ERC-1404 standard adds a function which allows the issuer to place transfer restrictions in a security token. However, the inclusion of a transfer restriction function does not necessarily mean that the transfer restriction can always be accurately triggered, because the criteria to trigger a transfer restriction is solely left to the issuer of the security token.[102] In other words, if an issuer can encode all the validation criteria necessary to meet the functional requirements under one of the offering exemptions, the added transfer restriction function can automatically prevent ineligible transfers. On the other hand, if the issuer inadequately or inaccurately encodes the validation criteria, the transfer restriction would not be properly triggered and consequently the token would not be compliance capable.

Thus, the success of the transfer restriction rest squarely on the ability of the issuer to properly code the validation function and the ability of the validation function to obtain accurate information in order to perform the validation. While some of the functional requirements stated above, such as cap on token supply, can easily be reliably performed, others such as obtaining the accreditation status of a potential buyer and their financial information would not be an easy task. Recall that Rule 506(c) requires issuers to "Take reasonable steps to verify that all purchasers are accredited investors," it is unclear what constitutes "reasonable steps" for a self-executing smart contract.[103]

Beyond the simple restricted token, there are currently other security token standards in the marketplace designed with an eye towards regulatory compliance.

(last visited March 1, 2019); *see also* Kenny Li, *Ethereum's ERC-20 Tokens Explained, Simply*, HACKERNOON, September 17, 2018, https://hackernoon.com/ethereums-erc-20-tokens-explained-simply-88f5f8a7ae90.

[100] See Peter Watts, *Beyond ERC20—A guide to non-standard Ethereum token functionality*, MEDIUM, February 15, 2018, https://medium.com/@ptrwtts/beyond-erc20-a-guide-to-non-standard-ethereum-token-functionality-bef5b9a9d457.

[101] SIMPLE RESTRICTED TOKEN STANDARD, https://erc1404.org/docs/readme.html (last visited March 1, 2019).

[102] The developers of the ERC-1404 standard listed several commonly implemented transfer restriction patterns such as Account Ownership Percentage, Account Holding Periods, Number of Accounts, Account Whitelists, or Token Divisibility, for example. *Id.*

[103] The duty to reasonably investigate investors actual financial condition and business sophistication "lay wholly" with the issuer; reliance on misrepresentation of the investors about their financial conditions can only be excused for an offering exemption only if such reasonable investigation has taken place. *Anastasi v. Am. Petroleum, Inc*., 579 F. Supp. 273, 275 (D. Colo. 1984). See discussion in footnote [83] for what constitutes reasonable effort to investigate.

First, Polymath's ST-20 token, formalized as ERC-1400,[104] adds requirements that tokens must be able to query off-chain data such as relevant documentation for the security.[105]

Harbor's R-token takes a similar approach in attempting to achieve compliance.[106] The R-Token has a function which contact a Regulator Service which will provide information regarding any proposed transfer.[107] If the Regulator Service validates that requirements are met, the transfer will proceed. On the other hand, if the Regulator Service cannot validate that requirements are met, the transfer will fail.

The premise of both ST-20/ERC-1400 and the R-token both require that the issuer develop the validation, the tokens are only providing the technical foundation to facilitate that. Harbor notes in its whitepaper: "The R-Token Standard provides an interface that developers can use to implement custom business logic. Harbor's planned implementations of the Regulator Service will include additional settings to enforce multi-jurisdictional requirements at a more granular Level."[108] In other words, having the capability does not necessary lead to utilization and compliance. This is evident by a recent study showing that many ICO issuers failed to implement on their tokens requirements which were promised during the offering process.[109]

How then, can a compliant-capable token be minted? The Compliance-Capable Token must be minted pursuant to a standard protocol which contains functional requirements which have been proven to be sufficient to meet regulatory scrutiny.[110] At first glance, this is difficult to assess before regulators and courts draw the lines on what constitute adequate investor protection. The Compliance-Capable Token Protocol should then be flexible enough that any token minted pursuant to the Protocol can be adjusted and deployed by an issue relying on any of above-mentioned offering exemptions. To achieve that, the Protocol must be capable of meeting all the functional requirements necessary under all the offering exemptions. Therefore, such a blockchain security token minted under the protocol must contain the following functions: (i) validation of potential buyer's residency jurisdiction; (ii) validation of potential buyer's

---

[104] ST-20 SECURITY TOKEN STANDARD, https://polymath.network/st20.html (last visited March 14, 2019).

[105] ERC 1400: Security Token Standard #1411, https://github.com/ethereum/EIPs/issues/1411 (last visited March 14, 2019).

[106] Bob Remeika, Arisa Amano & David Sacks, *The Regulated TokenTM (R-TokenTM) Standard*, February 6, 2018.

[107] *Id*. at 5.

[108] *Id*. at 8.

[109] *See* Shaana Cohney, David Hoffman, Jeremy Sklaroff & David Wishnick, *Coin-Operated Capitalism.*

[110] The crucial difference proposed here is that all the functional requirements be encoded on the token instead of relying on validation or logic residing off-chain at a third-party. In order for a *token* to be regulatorily compliant, *it* must be solely capable of performing the compliance validations. It is freely admitted that this may simply not be possible, as discussed *infra*, but adopting what is suggested here can possibly help prove that it can or as close to being achievable as possible.

accredited investor status, net worth, and annual income information; (iii) ability to impose resale restriction of the security tokens; and (iv) imposition of a maximum capacity of security token supply. Since intrastate offering is an impractical exemption, as previously discussed, function (i) can be disregarded. The remaining three functions must be implemented and enabled on any security token in order to meet any of the other offering exemptions.

Absent clear regulatory guidance, the following functions could be implemented to meet regulatory requirements as much as possible:

Resale Restriction. The security token must be capable of validating certain criteria before transfer of tokens can occur. Such validation may be based on a combination of criteria such as dates, amounts, and offering exemption the token was issued under.

Investor Screening. The token must attempt to establish the accredited investor status of a potential buyer, based on the investor's financial status, net worth, and annual income.

Rolling Offering Limit. As previously discussed, while total token supply can easily be calculated, it is not a reliable way to calculate the rolling aggregate total amount of offerings of a particular issuer because any issuer can issue multiple tokens unrelated to one another.[111] To prevent this, a Compliance-Capable Token must contain a function capable of identifying the issuer and calculating total token supplies minted by that issuer based on selected time periods. The Compliance-Capable Token must also contain a function defining which offering exemption the token is issue under so that the proper Rolling Offering Limit can be calculated.

Rolling Offering Limit. Similarly, the Compliance-Capable Token must contain a function capable of identifying the investor and calculating total investments the investor has made during a specific time period across all token offerings.

In summary, the Compliance-Capable Token must contain at least the following core technical functions in order to be capable of meeting the various offering exemption requirements:

Offering Exemption:	Which offering exemption the token is issued under
Investor Financial Screening:	detailed financial disclosure screening, dependent on the Offering Exemption
Issuer Identification:	Unique identification for a particular issuer across different token offerings
Total Supply Limit:	Total supply, capable of aggregate calculation based on Offering

[111] An issuer can issue $1million in Token A and $1million in Token B, each token individually can stay under the aggregate offering limit under Reg CF, but not when combined. See also discussion in note [90].

	Exemption, Issuer Identification, and transaction dates
Investor Identification:	Unique identification for a particular investor across different token offerings
Total Investment Limit:	Total investment amount, capable of aggregate calculation based on Offering Exemption, Investor Identification, and transaction dates
Resale Restrictions:	Restriction of transfer for a certain time period dependent on the Offering Exemption

With the foregoing core functions implemented, an issuer can clearly identify the offering exemption it is relying on, and the Compliance-Capable Token will enforce a set of smart contracts based on the exemption selection to ensure regulatorily compliant issuance and trading of the minted tokens. Of course, depending on future stances taken by regulators and courts, the protocol and the functions may be modified as needed thus evolving the Compliance-Capable Token Protocol.[112]

B. Alternative View: Token as a Technology

An alternate approach to implementing security tokens in an offering is to separate the token issuance from the securities issuance. In other words, issuers should conduct securities offerings as traditional non-blockchain offerings meeting traditional regulatory requirements, and only implement security tokens as digital share certificates on a distributed ledger.

Share certificates have undergone technological innovation. Gone are the paper certificates, replaced by registries maintained by the company or transfer agents, usually on digital ledgers.[113] The function of stock certificates is to evident ownership, so that when dividends are issued or shares are bought and sold, a chain of ownership can be established and buyers and sellers can be assured that they are transacting legitimate shares.[114] In a way, paper certificates were distributed ownership without a ledger. It allowed liquidity because they are easily tradable between willing buyers and sellers. However, the risk of fraud is great, and ledgers, in the form of ownership registries, were introduced to improve the accuracy and reliability of ownership evidence. In the process, the liquidity is diminished, as all transactions involving shares must be validated with the central share ledger.

---

[112] It is admitted that regulators and courts may ultimately determine that compliance functions cannot adequately be performed automatically on-chain. In such a case, the other two alternative views, discussed infra, can be relied upon to conduct regulatorily compliant token offerings.
[113] *See* Reyes, *supra* note [15].
[114] *See id*.

Moving to distributed ledger system will bring liquidity back without losing any of the security and reliability of a central ledger. In effect, A central ledger can still be utilized, but the operations of the ledger would be conducted on the distributed ledger first, then synchronized and recorded in the central ledger. Using this hybrid approach, investors can rely on the same protections offered by the central ledger while retaining the liquidity and flexibility offered by physical certificates. Here is where utilizing security tokens shines. Security tokens, once beyond the restricted period, could be bought and sold on the secondary market freely, utilizing smart contracts which enable efficient and almost instant transactions. With self-executing smart contracts, sales of security tokens can be performed in a very short period time–funds can be transferred, and token transfers can be settled instantaneously instead of two or three business days.[115] Additionally, the transaction is finalized and irreversible once it executes. Finally, there is little risk that the security token can be faked unlike physical share certificates. As long as the central ledger is properly synchronized with the distributed ledger, the central ledger will be kept up to date and accurate. The ease and efficiency offered by security tokens are not available through any existing trading systems.

The only potential concern rests with information disclosures about the underlying asset–the company whose fraction ownership interest are being bought and sold. If the security tokens were minted solely as a part of an ICO or STO, information disclosure depends on what was encoded into the security tokens by the issuer, which may be insufficient or inaccurate. However, if the offering was conducted as a traditional offering, compliant with all existing securities laws and regulations, the security token simply has to provide a link to the information disclosure made by the issuers through the traditional offering process.

Thus, deploying security tokens as technology is no different than issuing stock certificates in digital or electronic form, but at the same time offer a number of advantages.

The process of minting or issuing security tokens as technology is straight forward. First, an issuer conducts a traditional offering of securities fully compliant with existing securities laws, either through registration or pursuant to one of the offering exemptions. As a part of the sales process, the issuer obtains investor preference whether the investor wishes to hold the security in the form of security tokens.[116] The issuer will employ a central ledger for the purpose of the offering, recording all the initial purchasers of its securities onto the central ledger.

---

[115] SEC adopted a T+2 settlement cycle in 2017, which means standard broker-dealer securities transactions settle in two business days. *See* SEC Adopts T+2 Settlement Cycle for Securities Transactions, SEC Press Release 2017-68, March 22, 2017, https://www.sec.gov/news/press-release/2017-68-0.

[116] Similar to an issuer asking investors if they would like to have stock certificates issued.

Second, the issuer mints security tokens with three additional functional requirements beyond the customary security token functions: maximum number of tokens, resale restriction, and information disclosure link.[117]

Third, based on the investors' preference, the issuer transfers security tokens to investors who express desire to hold their own security tokens.

Fourth, the issuer creates individual accounts for all investors who do not wish to hold their shares in the form of security tokens, and transfer tokens representing those investors' shares to their respective accounts, still in the custody of the issuer.

Fifth, following the minting and transfers, the company's ledger keeper implements an automated process of synchronizing the central ledger with the decentralized ledger kept on the blockchain. In other words, subsequent transactions recorded on the blockchain should be recorded on the central ledger while transactions occurring off-chain will be performed on the blockchain from and subsequently recorded on the central ledger even for those security tokens still in the custody of the company. Because the blockchain ledger is transparent and immutable or irreversible, it can doubly serve as a trustworthy backup to the central ledger through this synchronization process.

At the conclusion of the initial minting and transferring process, investors who wish to hold their shares in the form of security tokens will have possession and custody of their security tokens, and the remainder security tokens belonging to investors not wishing to hold their security tokens are kept in the issuer's custody but allocated to those investors' accounts. If an investor shareholder changes their mind at a later time, their security tokens can be easily transferred to their address at that time from their account in the issuer's custody. Since blockchain is immutable, all initial and subsequent transfers are recorded and evidenced on the blockchain as well as the central ledger through the synchronization process and can easily prove the chain of title. Because all shareholders and all security tokens are recorded as a part of the initial offering, both the central ledger and the distributed ledger on the blockchain are complete and accurate.

Compared to making security tokens fully compliant, this hybrid approach of utilizing security token as technology supplements traditional securities offerings by enhancing the liquidity of the securities being offered. Such an advantage may increase the desirability and therefore the value of the securities. At the same time, since the underlying offering will be fully regulatorily compliant, the issuer can utilize blockchain technology without the uncertainties and risks that current ICOs and STOs face. Additionally, by employing the foregoing Compliance-Capable Token Protocol when issuing tokens, issuers can further ensure compliance of the distributed ledger in this approach.

---

[117] An issuer can of course implement the Compliance-Capable Token Protocol as discussed in the previous section.

C. Regulatorily Compliant Security Token Information Exchange

Under either approach described above, it is clear that compliance with securities laws and regulations can best be achieved through accurate information. Under the securities laws and regulations, on one hand, issuers are required to make accurate and sufficient disclosures to potential investors so they can make informed investment decisions; on the other hand, issuers are required to collect accurate financial information disclosure from potential investors so they can qualify for exempted offerings. The core of the disclosure requirement is designed to protect the investing public. Therefore, the more information an investor can easily obtain about an issuer and its securities, the better it is for the market.[118] With this goal in mind, it reasons that the investing public can benefit from a central place to obtain information about security tokens and their issuers.

One way to achieve this is the establishment of a regulatorily compliant Security Token Information Exchange. Despite being called an exchange, the proposed exchange does not have to directly facilitate trading. The primary goal is to facilitate information disclosure and exchange. The exchange can function fairly simply and efficiently. Since all transaction data are already reliably recorded on the blockchain, the exchange can organize the transaction data for each listed security token and display them in an organized way. As a matter of fact, similar blockchain information viewer already exists. At Etherscan, for example, one can browse or search through existing coins or tokens built on the Ethereum blockchain in real time, able to view any and all information about them.[119] A regulatorily compliant Security Token Information Exchange would then need two additional sets of information: issuer disclosures and investor disclosures. Issuers should be requested to make accurate disclosures to the exchange, but they are not required to. However, failure to make standardized disclosures will be marked as such, and potential investors will understand that there are higher risks associated with such an issuer. Investors will also be requested to make accurate disclosures about themselves, but similarly they are also not required to do so. For investors, disclosing the requested information can qualify them as accredited or sophisticated investors, following SEC defined procedures.[120] Once qualified, they can participate in appropriate offerings they are eligible to. Without making the disclosure and being qualified, investors will be barred from certain offerings where investor restrictions are in place.

Notably, blockchain can be utilized for both the issuers and investors disclosures. Issuers, the links to their disclosures, as well as investors and their

---

[118] An efficient market is one where market price of securities fully reflects all publicly available information, and a lack of information efficiency would result in greater price volatility. *See* Robert G. Newkirk, *Sufficient Efficiency: Fraud on the Market in the Initial Public Offering Context*, 58 U. CHI. L. REV. 1393, 1411 (1991).

[119] Etherscan, https://etherscan.io/, last visited March 1, 2019.

[120] Updated Investor Bulletin: Accredited Investors, SEC, January 31, 2019, https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/updated-investor-bulletin-accredited-investors.

qualification status can all be recorded on the blockchain, each with unique identifiers. Doing so helps solve the challenges discussed earlier relating to Rolling Offering limits and Rolling Investment Limits.

The proposed exchange can further be approved as a third-party intermediary qualified to conduct Regulation Crowdfunding offerings through registration with SEC. As a matter of fact, the proposed exchange seems to embody the purpose and goal of regulated crowdfunding portals-crowdfunding portals are permitted to list Regulation Crowdfund offerings without offering investment advice, thus only provide information about the offerings.[121] The proposed exchange can function in the same way, providing accurate information about security tokens without providing any investment advice or rating the offerings in anyway.[122]

Having such an exchange also reduces the burden of regulators. Regulators require accurate data in order to monitor the marketplace and ensure compliance. Due to the nature of the blockchain, all the data about all the security tokens will be available, accessible, and accurate for the regulators to review. Additionally, all the data about all the issuers and investors who opted-in by making accurate disclosures will also be available, accessible, and accurate. Regulatory agencies can obtain all the data they need to ensure compliance easily and without hurdles. Issuers do not even need to make additional specific disclosures to the regulators because all the disclosures necessary are plainly available on the blockchain and on the exchange. Through the provision of information disclosure, the proposed exchange would enhance both of the approaches previously discussed in this article.

VI. CONCLUSION

Self-regulation is the traditional and frequently preferred method of regulating financial industry unless fraud and abuse forces direct governmental intervention.[123] A new industry can meaningfully influence legislation and regulation if it can show regulators that preliminary or initial self-regulation has proven to be effective in regulating the market.[124] Unfortunately, so far the cryptocurrency and ICO markets have screamed the need for regulation. It is wise for the blockchain community to band together and self-regulate in a meaningful way before undesirable regulation is imposed upon the marketplace. Even if governmental intervention, through SEC or other regulatory agencies, is inevitable, meaningful and effective self-regulation practices would not be totally

---

[121] *See* Crowdfunding, Exchange Act Release Nos. 33-9974, 34-764324.

[122] Providing investment advice or rating information would necessitate the proposed exchange registering as a broker-dealer. *See id*.

[123] The Supreme Court opined in *Silver v. New York Stock Exchange*, 373 U.S. 341, 351-352 (1963), that government regulation of national exchanges grew out of the financial industry's "inability and unwillingness to curb abuses" but the government did not intent "total displacement of the exchanges' traditional process of self-regulation."

[124] *Id.*

displaced. In other words, the blockchain industry has an opportunity to write the rules it wants to be governed by before it is too late. Minting compliance-capable security tokens, conducting offerings compliant with existing securities laws and regulations, and establishing an information exchange as suggested by this article, are all meaningful steps for the blockchain industry to illustrate its ability to meaningfully self-regulate and dictate its regulatory future.

The security token industry is in its infancy. ICOs and the fast and loose money that funded them are likely a thing of the past. In order for blockchain technology to survive and thrive in the long run, regulations are needed to protect both the investors and the fragile new technology sector. With proper regulatory guidance and industry buy-in, DLT, blockchain, and security tokens can continue to revolutionize the way we view, hold, and transfer ownership, for virtually any valuable asset.