The SEC meditates on The DAO: tracing the initial arc of cryptosecurities regulation

Aegis Frumento and Stephanie Korenman

Aegis Frumento (afrumento@sterntannenbaum.com) and Stephanie Korenman (skorenman@sterntannenbaum.com) are co-heads of the Financial Markets Practice of Stern, Tannenbaum & Bell, LLP, New York, New York, USA.

Abstract

Purpose – *The purpose of this paper is to review the first two years of the US Securities and Exchange Commission (SEC) efforts to regulate cryptosecurities to assess the trends of that regulation.*

Design/methodology/approach – *The authors review the SEC's official pronouncements and informal statements about, and its enforcement actions against participants in, various early experiments in cryptosecurities.*

Findings – *The SEC has been evolving how to apply the US securities laws to cryptosecurities since its report on The DAO two years ago. When "coins" on a blockchain meet the traditional Howey Test, it is easy to categorize them as "securities." However, the bedrock regulatory principle that some person must account for violations is frustrated by automated blockchain transactions, where no human is in control. This tension risks a "moral crumple zone" arising around cryptosecurities, in which persons might become liable for violations that they cannot fairly be said to have caused.*

Originality/value – *This paper provides valuable information and insights about the beginnings of US regulation of cryptosecurities and how the evolution of that regulation is trending after two years.*

Keywords *Blockchain, Cryptosecurity, The DAO, Utility token, Moral crumple zone, US Securities and Exchange Commission (SEC)*

Paper type *Technical paper*

1. Introduction

Last year, Sarah Douglas, seven months pregnant, ordered a latte from a McDonald's drive-through. As she drove away, she took one sip – and spit it out. Turns out, it was laced with cleaning fluid. Fortunately, she didn't drink the rest of it, and she and her baby were unhurt[1]. Admittedly, that was a random event. But take it a step further: What if you hand a five-dollar bill to a Starbucks barista and order a half-caf, skinny vanilla latte? One can tell cleaning fluid, but is yours really half-caf? Did they use low-fat milk? Did they use sugar-free vanilla syrup? How could you ever really know?

You can't. You have to trust there was no whole milk or sugar in your latte, just as the barista has to trust that you didn't pay for it with a counterfeit bill. Even this simplest exchange of food for currency could not happen if you and the barista did not trust each other. Social life – economic life – cannot exist without trust. Because trust is so essential, promoting trust and punishing breaches of trust are what the law is mostly about. Lawyers call it *negligence* when trust fails due to carelessness and *fraud* when it is intentional. All securities law aims to prevent the former and deter the latter.

In the wake of the Great Credit Crash, one could argue that trust in financial institutions crashed the hardest. In Fall 2008, a pseudonymous coder named "Satoshi Nakamoto" decided that financial institutions could no longer be trusted. He/she/they published a white paper proposing a method for processing financial transactions without relying on trusted third parties to execute and record them – the blockchain. Blockchain is literally that – a

Editor's Note: Portions of this article first appeared in various essays by Aegis Frumento posted online at www.BrokeAndBroker.com, and archived at www.brokeandbroker.com/index.php?a=topic&topic=aegis-frumento

chain of blocks. Each "block" contains digitally encrypted information about transactions, and each block is cryptographically linked to those adjacent to it to form a "chain." The chain of blocks is publicly accessible, so anyone can verify the integrity of the transactions it encodes. Satoshi proposed using a blockchain to instantiate "bitcoin," a digital currency – electronic cash secured by the blockchain instead of any central bank.

On January 3, 2009, the very first block of transactions – the so-called "genesis block" – was validated on the Bitcoin blockchain. Rarely can we date the birth of a new technology so precisely. From its beginnings, bitcoin was hailed as the next evolution of money, independent of governments, banks and other centralized institutions of trust (and, necessarily, of control). Some predicted that financial institutions would soon become obsolete. Venture capitalist Naval Ravikant tweeted, "Bitcoin is a tool for freeing humanity from oligarchs and tyrants, dressed up as a get-rich-quick scheme"[2]. But most have focused on the "get-rich-quick" part, leading naysayers like Nobel Prize-winning economist Paul Krugman to label bitcoin "evil"[3].

2. What is blockchain?

Few have a good understanding of how blockchain technology works or why it is so powerful. Because blockchain is so unlike anything that we are already familiar with, it is devilishly difficult to describe to the uninitiated. There are several good books on the subject, but they are not light reading[4]. The Financial Industry Regulatory Authority (FINRA) put out a primer that's as good as any[5]. But because blockchain technologies are so little understood, they have become a common vehicle for fraud in recent years[6].

The blockchain is simply a way of recording transactions in a publicly accessible ledger, using cryptographic techniques that ensure the ledger can never be tampered with and so will always be accurate. There is no centralized server, as there would be for a conventional ledger. Rather, the transactions are broadcast throughout a network of computers and the blockchain in which the transactions are recorded exists in multiple copies across the network. This "decentralization" makes the information difficult to manipulate, and as the number of copies of the blockchain in the network increases, the probability of manipulation drops to near zero. In the case of bitcoin, the Bitcoin blockchain exists in so many places[7] that so far no one has succeeded in hacking it[8].

Like a bank statement or a checkbook, the blockchain contains records of transfers of things in and out of particular accounts, and the resulting balances. Transfers are effected through two mathematically related cryptographic keys, one public and one private. You can freely give away your public key, but your private key is yours alone. Anyone with your public key can transfer a thing on to your ledger, but only you, with your private key, can transfer a thing out. If A wishes to transfer 100 bitcoin from her account to B's account, she uses her private key to effect the transfer, and B's public key to identify the destination. If the keys are authentic, A's ledger is decreased by 100 bitcoin and B's ledger is increased by 100 bitcoin[9]. The debit and credit occurs automatically, with no human involvement or interference. Owners of bitcoin generally transact through websites known as coin exchanges that have direct access to the Bitcoin blockchain. There are several dozen coin exchanges on which various cryptoassets can be traded; accounts held on coin exchanges are called "wallets."

What makes a blockchain different than conventional ledgers is that they are (in theory) tamper-proof[10]. Once validated by whatever validation method the blockchain adopts [11], the transaction cannot thereafter be changed. The blockchain software will simply not recognize any attempt to change a valid transaction, so it just never happens. The blockchain thus ensures that once A transfers a coin to B, (a) that coin ends up in B's account, (b) A cannot transfer that coin a second time to anyone else, and (c) only B can transfer that coin (and then only once) to someone else. Those are all that it means to "own"

something. In theory, a blockchain-based ledger makes account errors, misdirected funds, ledger tampering and embezzlement so difficult as to be deemed practically impossible. No trust in any person or institution is needed to ensure ownership of whatever the blockchain tracks, bringing us full arc to Nakamoto's original premise.

3. What is a cryptosecurity?

Whatever can be counted and transferred can be tracked on a blockchain[12]. Any such thing is now conventionally represented by a "coin" if it is a financial thing, and a "token" if it is a non-financial thing. But not all coins are currency and not all tokens are non-financial objects. Equity interests in business ventures – what we now call stocks – can also tracked on a blockchain, and have also been called variously coins or tokens. This confusing nomenclature more than anything has driven the past two years' developments in cryptosecurities. Odd as it seems, the regulation of cryptosecurities is evolving from the misguided efforts of promoters thinking that what they were peddling fell outside the securities laws just because they were called "coins" or "tokens" instead of stock or bonds.

It did not take long to realize that a blockchain could do more than bookkeeping. In the mid-1990s, software engineer Nick Szabo first articulated how to write a software routine that executes legally valid transactions automatically when certain events occur – a "smart contract"[13]. In 2015, Ethereum launched a blockchain designed to implement smart contracts, using its cryptocurrency, ether, as the medium of exchange[14]. The availability of blockchain-enabled smart contracts led to the idea of a distributed autonomous organization, a DAO. A DAO is a virtual company run by algorithms executed entirely by smart contracts on a blockchain, rather than by human management. The smart contracts of a DAO execute transactions on a blockchain according to their code, to fund projects, collect revenues, pay expenses, and distribute profits, all without centralized human control. In theory, with no central authority to alter transactions recorded in a blockchain, DAO smart contracts executed through the Ethereum blockchain should completely impregnable.

In May 2016, Slock.it, a blockchain developer in Germany, set up a DAO brilliantly called "The DAO." The DAO raised about $150 million selling DAO tokens in exchange for Ethereum's cryptocurrency, ether. Glossing over the mechanics, The DAO's capital was intended to be deployed to fund various curated projects as determined by votes of The DAO's token-holders. Once projects were chosen, The DAO would monitor project results, collect profits, and distribute them to its token-holders without centralized control. In essence, The DAO would be an automated investment fund, with little or no administration behind it[15].

But before The DAO could fund any projects, someone now known only as "The Attacker" exploited a feature of The DAO's smart contract code to divert a third of The DAO's assets to their own account. Slock.it and Ethereum eventually found a controversial way around The Attacker to recover the assets[16], but the episode gave the U.S. Securities and Exchange Commission the impetus for a first critical analysis of blockchain-based securities. The result was a fundamental review of what is a "security" under the federal securities laws[17]. The SEC's regulation of cryptosecurities begins with The DAO.

In one sense, the SEC's Report on The DAO was too fundamental. After noting the trend to raise capital through events called "Initial Coin Offerings" or "Token Sales," the SEC warned that "the U.S. federal securities law may apply to various activities, including distributed ledger technology, depending on the particular facts and circumstances, without regard to the form of the organization or technology used to effectuate a particular offer or sale"[18]. This is true "regardless of the terminology used"[19]. Going back to what is known as the *Howey* Test, after the seminal U.S. Supreme Court case that first enunciated it in 1946[20], the SEC defined a security as "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"[21]. Given that definition, the SEC handily concluded that The DAO's tokens were securities and that The DAO was itself an "issuer" obligated to register its token sales.

4. What are (maybe) not cryptosecurities?

Since then, the SEC has continued to refine incrementally, typically by enforcement actions, when a coin or token is a cryptosecurity subject to regulation. By and large, the SEC has had little difficulty recognizing most coin and token offerings as securities[22]. However, there are three noteworthy exceptions.

4.1 Currency

Coins and tokens that are primarily media of exchange do not fit the definition of a "security," because they are not held with an expectation of profit from the efforts of others. So far, only bitcoin and ether are generally recognized as pure currency, with no securities law implications to owning or trading them. No one will usually buy a new cryptocoin without some reason to think there will be a profit from someone's economic activity, so the *Howey* Test is usually met. SEC Chairman Jay Clayton has expressed his view that any cryptoasset could become a currency once holding it no longer carries a promise of profit from the work of others[23]. But it seems clear that very few newly issued-coins or tokens could be deemed currencies from their inception.

However, a derivative instrument that is based on a currency would be a security. There have been several attempts, none yet successful, to obtain SEC approval for an exchange-traded fund (ETF) that holds bitcoin. Several SEC commissioners have gone on record that they expect a bitcoin ETF will be approved eventually, but only after concerns over market volatility and manipulation are addressed[24]. The issue was first raised in a January 2018 staff letter, in which Dalia Blass, the Director of the Division of Investment Management, pointed out that to be approved, a cryptocurrency ETF must be able to accurately value its assets to establish a net asset value (NAV), must be able to liquidate its assets quickly to meet redemption demands, and must trade during the day at close to their NAV to avoid manipulative arbitrage[25].

One of the first attempts at a bitcoin ETF was the Winklevoss Bitcoin Trust. The SEC rejected that application in July 2018, giving many examples of how bitcoin markets could be and had been manipulated. It then went on to conclude that the Trust had not demonstrated its assertion that bitcoin trading "generally is less susceptible to manipulation than the equity, fixed income, and commodity futures markets"[26]. The SEC recently denied a request to form a bitcoin ETF by Bitwise Asset Management. Bitwise argued that "Bitcoin is a globally fungible commodity with low transaction costs, near-zero transportation costs and low-to-zero storage costs." For those reasons, according to Bitwise, "you would expect a bitcoin market to be uniquely orderly and efficient, with tight spreads and nearly perfect arbitrage." Yet, after analyzing the trading in bitcoin on 81 coin exchanges, Bitwise concluded that only 10 of them exhibited trading patterns that met those expectations. The rest of the coin exchanges, 87 per cent of them, did not, corroborating the SEC's conclusion about the overall turbulence of bitcoin markets. Bitwise then supported its application by, in effect, promising only to track its NAVs against the 10 "real" exchanges[27]. Not surprisingly that gambit failed. As of this writing, only one bitcoin ETF application remains pending[28].

4.2 Utility Tokens

In the simplest terms, a token is a stand-in for cash, designed to be more useful for its purpose than cash would be. Amusement park coins, poker chips and postage stamps are all tokens. They are as good as money, but only for their intended purpose. By that definition, they should be considered proxies for currency, and thus not securities. Turnkey

Jet, Inc. (TKJ), a company that leases private business jets, set up a private blockchain and issued tokens to its members. TKJ's members include end-users, jet brokers, and other air transport companies. Each TKJ token is worth a dollar and can only be used to pay for air charter services; they are not an investment in TKJ itself[29]. Given all that, the SEC had no trouble issuing a no-action letter allowing TKJ to issue its tokens without registering under the securities laws[30].

TKJ presented the cleanest and easiest example of a pure token, clearly not a security. In the wake of The DAO Report, many crypto-promoters started to give their coins some utility beyond mere profit potential, and argued that utility meant it was not a cryptosecurity. The SEC got wise to that early on. In a public statement issued just five months after The DAO Report, Chairman Clayton expressly called attention to utility tokens. "Merely calling a token a 'utility' token or structuring it to provide some utility does not prevent the token from being a security." If utility tokens also carry – and are marketed to highlight – potential passive profits, then more likely than not they will be deemed securities[31]. TKJ's tokens expressly disclaimed any profit potential from TKJ's business, so they easily passed muster.

4.3 Beta Tests that look like ICOs

This is perhaps the most intriguing possible exception. A venture called Blockvest "pre-sold" 9 million blockchained tokens, called "BLVs," to 32 buyers for roughly $180,000. The SEC sued to enjoin what it saw as an unregistered ICO. But Blockvest argued that, appearances notwithstanding, the BLVs it had issued were not securities, because the 32 buyers did not expect to make a profit from them. Blockvest's BLVs embodied a smart contract that would execute automatically through the blockchain. Therefore, the BLVs were themselves operational pieces of computer software that needed to be tested in the actual operating environment, by actual users, in what is called a beta test. Blockvest argued that beta testing the BLVs meant they had to be bought by real people using real money. Those purchases would be indistinguishable from investments, except for the mental expectations of the purchasers. Blockvest presented evidence that the BLVs it pre-sold were not bought by investors expecting to make a profit, but by a select group intending to test the Blockvest system. Without a profit expectation, the BLVs would fail the *Howey* Test, and so the district court found[32].

5. What are cryptosecurities broker-dealers and exchanges?

The next set of issues with which the SEC is starting to grapple is not as clear as asking whether a particular coin or token is a cryptosecurity. When are the side-participants in a blockchain ecosystem acting as broker-dealers and securities exchanges? The answers are less satisfactory because they are artificially constrained by the definitions of the securities laws. Basically, once one concludes that a particular coin or token is a security, then anyone who brokers, deals in or facilitates a transaction in that coin or token is naturally included in the existing definitions of a securities broker-dealer or exchange. However, those side players do not necessarily operate in relation to a blockchain the same way their traditional analogues do with respect to conventional securities.

Part of the problem arises because the securities laws are built on the assumption that some person must be held accountable for errors in handling securities transactions. Chairman Clayton has more than once highlighted personal accountability as one of the pillars of securities regulation[33]. But as we have seen, a fundamental goal of blockchain-enabled transactions is to remove humans from the transaction process. A perfect example of how ill-fitting traditional regulations are when they are applied to cryptosecurities arose in the question-and-answer segment of Chairman Clayton's interview with Andrew Ross Sorkin of *The New York Times*. A member of the audience asked why a private offering of cryptosecurities must identify a transfer agent. A transfer agent will be responsible for

ensuring that privately issued securities are not improperly distributed to the public. However, as the questioner pointed out, a cryptosecurity does not need a transfer agent, because the blockchain itself ensures that it cannot be transferred to someone who is not legitimately authorized to own it. Any attempt to do so would just fail. Why, then, would the regulations require the identification of a transfer agent who will have nothing to do? Chairman Clayton, rather than answer the question, asked rhetorically who, if there were no transfer agent, would be held responsible if the cryptosecurity did escape into public ownership? He and the questioner were talking perfectly past each other[34]. That exchange illustrates an underlying issue in the SEC's efforts to impose securities law liability on collateral participants in cryptosecurities transactions.

This is more relevant in some matters than in others. Undoubtedly, a broker or dealer in cryptosecurities owes the same duties to customers as do all brokers and dealers. While most holders of cryptosecurities do not act through brokers or dealers, there are exceptions. The SEC's case against TokenLot proves the point. According to the SEC Release, "TokenLot's business primarily consisted of selling digital tokens in connection with both ICOs of other entities and secondary market trading, and marketing digital tokens on behalf of issuers." TokenLot called itself an "ICO Superstore[35]". Admittedly it is hard to say it was not acting as a broker-dealer.

It is less clear that a coin exchange should need to register as a securities exchange. EtherDelta was a blockchain enabled platform that allowed holders of some cryptosecurities to trade them, using a front-end trading screen very much like any other stock trading screen. EtherDelta performed all the typical functions of an exchange, including quote display, order matching and trade execution. The SEC easily concluded that it performed all the key functions of a securities exchange, and should have registered as such[36]. And yet, EtherDelta did not operate like a traditional exchange, because, as the SEC acknowledged, "EtherDelta's business operations are defined and executed by EtherDelta's 'smart contract' that runs on the Ethereum Blockchain. The EtherDelta smart contract consists of coded functions that allow for, among other things, the trading of any Ether/ERC20 token pair[37]". In other words, no humans (or human-controlled entities) controlled EtherDelta's operations[38].

6. Conclusion

Like Chairman Clayton's response to the question about unnecessary transfer agents, the EtherDelta case is another example of the traditional need of securities law to hold someone accountable even in the face of a blockchain technology that seeks to remove personal accountability altogether. It raises the broad question of who should be liable when no one is really responsible. This is not new in the law. Traditionally no one is deemed responsible for natural disasters and other so-called "acts of God." The solution to those catastrophic events is not personal liability, but insurance.

Interestingly, one of the elements of the *Howey* Test is that profits be expected from the efforts of others, and those "others" are implicitly human actors. The SEC recently acknowledged as much, noting that the prong of the test is met when some "Active Participant" "provides essential managerial efforts that affect the success of the enterprise, and investors reasonably expect to derive profits from those efforts"[39]. One suggestion is that the more ministerial the work of the Active Participant, the less likely that investors are relying on that work in expecting a profit. But so far, enforcement actions have snared many whose active participation seemed limited to setting up and launching a blockchain-based coin or token. It is hard to see how an investor could expect to profit from someone with no ability to control the blockchain on which their newly minted cryptocoins would be tracked. And yet, that seems to be the arc of cryptosecurities regulation.

Research has noted a tendency to blame a human – any human – who happens to be close by when technology goes awry. Studying failures in automated systems, such as the Three Mile Island nuclear accident and the crash of Air France 447, researcher Madeline Clare Elish notes that although automated system failures caused the accidents, the media and public were quick to misattribute blame to the humans who were close by. There are "contradictory dynamics in which automation is seen as safer and superior in most instances, unless something goes wrong, at which point humans are regarded as safer and superior." Then, humans become the "moral crumple zone"[40]. Like the car frame that absorbs the shock of a crash to protect the human, the human bystander to an automated system absorbs the moral blame that we can't well impose on the machine.

A moral crumple zone does not explain why cryptosecurities regulation since The DAO Report is evolving towards imposing liability on persons who cannot logically be deemed responsible for blockchain errors. The simpler explanation is that once having passed the *Howey* Test, cryptosecurities become the basis of collateral liability for any who deal in them. This follows naturally from applying current statutory definitions and traditional legal concepts to a technology that was unknown when those were first formulated – and applying them no matter how ill the fit. Nor does a moral crumple zone require this result. But a moral crumple zone well describes what cryptosecurities law will look like if existing securities laws are not revised to better address the autonomous – non-human – operations at blockchain's core.

Notes

1. *Pregnant mom served cleaning solution instead of latte at southern Alberta McDonald's* (July 31, 2018), available at www.cbc.ca/news/canada/calgary/lethbridge-pregnant-mother-sarah-douglas-mcdonalds-latte-cleaning-1.4769286
2. Available at https://twitter.com/naval/status/955998687670411264
3. *See, e.g.*, Paul Krugman, *Bitcoin is Evil* (Dec. 28, 2013), available at http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/
4. *See, e.g.*, Arvind Narayanan, *et al.*, BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES (2016); Kevin Webach, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST (2018); Primavera De Filipi & Aaron Wright, BLOCKCHAIN AND THE LAW (2018); Reade Ryan & Mayme Donohue, *Securities on Blockchain*, 73 BUS. LAWYER 85 *et seq.* (Winter 2017-2018); Primm (2016/2017).
5. FINRA, *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry* (Jan. 2017), available at www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf
6. One of the most spectacular was a global Ponzi scheme based on a fake cryptocurrency called OneCoin, which bilked naïve "investors" of over 3 billion euros over several years, despite warnings from bank regulators and prosecutors in a dozen countries. *See* www.justice.gov/usao-sdny/press-release/file/1141986/download and www.justice.gov/usao-sdny/press-release/file/1141981/download. *See also,* Frumento (2019a).
7. Anyone can download the Bitcoin ledger and enabling software. *See* https://bitcoin.org/en/download
8. It is widely believed that the vastly greater computational power of quantum computers could hack a blockchain, but such computers are not likely to appear for some time.
9. We've used a transfer of bitcoin as an example because we instinctively think in terms of physical things like coins and talk of "transferring" them. But no physical thing happens. Rather, at the end of transaction, both A and B have a certified number of "unspent transaction outputs," counted in bitcoins, A's being 100 less and B's 100 more than before. What B has actually acquired is the power to transfer 100 bitcoins to someone else.
10. Why they are tamper-proof requires a discussion of their data structures (blocks, chains and Merkle Trees) and verification methods ("mining"), which is beyond our scope in this article. See the references in Note 4 and 5 *supra*, and 13 *infra* for more information. This is where you'll have to trust us.

11. Bitcoin "mining" is one method of validation. It is a complex ritual by which keepers of the Bitcoin blockchain compete against each other to add blocks to the blockchain. Each miner collects pending bitcoin transactions into a cryptographically related "block," and then search (using mathematical processes) for the one number (called the "nonce") that allows that block to be appended to the existing blockchain. That number found, the miner broadcasts it to the blockchain, and when 51 per cent of the blockchain servers verify the proposed block has the proper nonce, it is added to the blockchain and all the transactions in that block are then validated. The miner gets paid because one of the transactions in the just-validated block added bitcoin to the miner's account as the miner's reward, which is effected once the block is validated. This is the "proof of work" model. *See generally* Arvind Narayanan, *et al.*, BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES (2016), at 104-105. There are others. *See, e.g.,* the Libra White Paper referred to in note 21 *infra*.
12. In a dramatic example of the power of blockchain ledgering, Walmart recently demonstrated how the source of contaminated lettuce, when tracked on a blockchain, can be identified in seconds, when conventional tracking methods would need a week. *In Wake of Romaine E. coli Scare, Walmart Deploys Blockchain to Track Leafy Greens* (Sept. 24, 2018), available at https://news.walmart.com/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens. Each head of lettuce in this case is a countable thing that can be proxied by a coin. Its transfer from farm to packing company to wholesaler to shipper to warehouse to store can be recorded on a blockchain as if it were bitcoin. Since the blockchain record of the last transfer embeds all prior transfers back to the original source, locating that source becomes fast and easy.
13. *See* Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (original 1994, rewrite 1996), available at www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html; Nick Szabo, *Formalizing and Securing Relationships on Public Networks* (Sept. 1, 1997), available at https://ojphi.org/ojs/index.php/fm/article/view/548
14. *See* www.ethereum.org/
15. *See generally*, Christoph Jentzsch, *Decentralized Autonomous Organization to Automate Governance Final Draft – Under Review,* https://download.slock.it/public/DAO/WhitePaper.pdf
16. This involved creating a "hard fork" that split the Ethereum blockchain in two, where the new blockchain did not recognize The Attacker's transaction. *See Ethereum Classic vs Ethereum (ETC vs ETH): What's the Difference?* (Apr. 22, 2019), available at https://coincentral.com/ethereum-classic-vs-ethereum/. This was controversial because it violated a core principle of blockchain, that transactions done cannot be changed. A minority of Ethereum users will not recognize the new Ethereum and will only use what is now called Ethereum Classic. According to them, what happened, happened, and people should live with the consequences. *Ethereum Classic*, available at https://ethereumclassic.github.io/. *See also*, Frumento (2019b).
17. SEC Rel. No. 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (July 25, 2017), available at www.sec.gov/litigation/investreport/34-81207.pdf
18. *Id.* at 10.
19. *Id.* at 17.
20. *SEC v. W.J. Howey Co.,* 328 U.S. 293, 301 (1946).
21. *SEC v. W.J. Howey Co.,* 328 U.S. 293, 301 (1946) at 11, *citing SEC v. Edwards,* 540 U.S. 389, 393 (2004); *United Housing Found., Inc. v. Forman,* 421 U.S. 837, 852-53 (1975); *Tcherepnin v. Knight,* 389 U.S. 332, 336 (1967); *SEC v. W.J. Howey Co.,* 328 U.S. 293, 301 (1946).
22. *See* recap at SEC (2018).
23. *See* interview of Chairman Jay Clayton with *The New York Times's* business columnist Sorkin (2018).
24. *See* remarks of Chairman Clayton (2018); *see also* remarks of Commissioner Jackson (2019).
25. SEC *Staff Letter: Engaging on Fund Innovation and Cryptocurrency-related Holdings* (Jan. 18, 2018), available at www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm
26. *See* Release No. 34-83723 (July 26, 2018), available at www.sec.gov/rules/other/2018/34-83723.pdf
27. *See* Bitwise Asset Management, Inc., Presentation to SEC (2019a).

28. As of this writing, a consortium led by Facebook announced their own cryptocurrency, the Libra. Unlike bitcoin, the Libra will be controlled by a central authority (The Libra Association) and will be backed by hard currency, $10 million each contributed by the Association's proposed 27 members. These will in theory make the Libra scalable, fast and stable. *See* https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf. Libra essentially does away with the anarchy of the original bitcoin model. It is in many ways the very opposite of bitcoin, a bold assertion that a decentralized blockchain cannot spawn a real "currency." See also, Frumento (2019c).
29. The TKJ token's attributes are set forth in its no-action letter request to the SEC (2019b).
30. SEC No-Action Letter, *TurnkeyJet, Inc.* (Apr. 3, 2019), available at www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm
31. Jay Clayton, *Statement on Cryptocurrencies and Initial Coin Offerings* (Dec. 11, 2017), available at www.sec.gov/news/public-statement/statement-clayton-2017-12-11
32. *SEC v. Blockvest, LLC, et al,* 3:18-cv-02287-GPC-MSB (S.D. Ca., Nov. 27, 2018)(Doc. No. 41), available at www.fintechupdate.com/wp-content/uploads/sites/20/2018/12/SEC-v-Blockvest.pdf. The Court later granted the SEC an injunction on reconsideration, not because the BLVs were not beta tests, but because the Blockvest white paper constituted an unregistered "offer" of securities. *See id*, Doc. No. 61 (Feb. 14, 2019), available at www.sec.gov/litigation/litreleases/2019/order24400.pdf
33. *See* especially the interview at *supra* note 23.
34. *Id.*
35. *Matter of TokenLot, LLC, et al.,* Admin. Proc. 3-18739 (Sept. 11, 2018), available at www.sec.gov/litigation/admin/2018/33-10543.pdf
36. *Matter of Zachary Coburn*, Admin Proc. 3-18888 (Nov. 8, 2018), available at www.sec.gov/litigation/admin/2018/34-84553.pdf
37. *Id.* at 4.
38. Similar issues arise when speaking of "custody" of cryptosecurities to satisfy the broker-dealer financial responsibility and customer protection requirements of SEC Rules 15c3-1 and 15c3-3. Cryptosecurities are not physical things for which "custody" has any real meaning. One has custody of a cryptosecurity by knowing the password that permits it to be transferred on the blockchain. "Custody" of a cryptosecurity, then, really involves password security and recovery procedures. This was highlighted in the catastrophe faced by Canada's largest coin exchange, QuadrigaCX, which filed for bankruptcy when its founder died and no one could recover the password needed to access $140 million in ether it held for its customers. *See Cryptocurrency customers are unable to access their coins after Canadian CEO's death* (Feb. 4, 2019), available at www.cnbc.com/2019/02/05/millions-in-cryptocurrencies-frozen-after-quadriga-founders-death.html. *See also* Aegis J. Frumento, *To Hold and Have Not* (Feb. 14, 2019), available at www.brokeandbroker.com/4438/aegis-frumento-quadrigacx/. The SEC is only beginning to grapple with this issue, but in doing so it faces the same problem of applying ill-fitting legal concepts to new realities. *See Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities* (July 8, 2019), available at www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities
39. SEC, *Framework for "Investment Contract" Analyses of Digital Assets* (Apr. 3, 2019), available at www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets
40. Madeleine Clare Elish, *Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction* (Mar. 1, 2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757236

References

Clayton, J. (2018), available at: www.coindesk.com/clayton-sec-ico-funding-security-offering

Frumento, A.J. (2019a), "OneCoin's whorl of woe", available at: www.brokeandbroker.com/4473/aegis-frumento-onecoin/

Frumento, A.J. (2019b), "The hard fork in DAO road", available at www.brokeandbroker.com/4412/aegis-frumento-dao/

Frumento, A.J. (2019c), "The great pretender", available at: www.brokeandbroker.com/4664/aegis-frumento-libra/

Jackson, R.J. Jr. (2019), available at: www.theblockcrypto.com/tiny/bitcoin-etf-will-see-eventual-approval-sec-commissioner-says/

Primm, H. (2016/2017), "Developments in banking law", *Review of Banking & Financial Law*, Vol. 36, pp. 75-80.

SEC (2018), "SEC divisions of corporate finance, investment management and trading & markets, statement on digital asset securities issuance and trading", available at: www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading

SEC (2019a), available at: www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf

SEC (2019b), available at: www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1-incoming.pdf\

Sorkin, A.R. (2018), available at: www.youtube.com/watch?v=YVekxba40ZQ

Corresponding author

Aegis Frumento can be contacted at: afrumento@sterntannenbaum.com