Tennessee Law Review

Volume 85
Issue 4 *Summer 2018*

Article 3

2018

THE NEW DIGITAL WILD WEST: REGULATING THE EXPLOSION OF INITIAL COIN OFFERINGS

Randolph A. Robinson II

THE NEW DIGITAL WILD WEST: REGULATING THE EXPLOSION OF INITIAL COIN OFFERINGS

RANDOLPH A. ROBINSON II*

INTRODUCTION 899
I. OVERVIEW OF DECENTRALIZED LEDGER SYSTEMS 904
A. *Big Picture: The Shift to a Decentralized World* 905
B. *What Is the Blockchain?* 908
C. *How the Blockchain Works* 911
D. *The Ethereum Platform* 919
II. INITIAL COIN OFFERINGS 924
III. THE SEC'S REPORT ON THE DAO 929
A. *The DAO* 930
B. *Howey* 934
C. *Investment of Money* 934
D. *Common Enterprise* 935
E. *Expectation of Profits from the Efforts of Others* 940
IV. POST-DAO REPORT DEVELOPMENTS 948
A. *The Move to "Utility Tokens"* 950
B. *SEC's Early Enforcement Actions Against Token Issuers* 952
V. RETHINKING THE REGULATORY FRAMEWORK 955
A. *The SEC's Limited Enforcement Ability* 955
B. *Endogenous Regulation as a Path Forward* 956
C. *Creating a Safe Harbor Through Code as Law* 957
CONCLUSION 960

In less than a calendar year, initial coin offerings or "ICOs" have become the fastest growing capital market in the world. In 2016, an entity called The DAO raised $160 million by selling crypto-tokens to over 15,000 individual purchasers around the globe. This massive fund raise would give rise to an entirely new capital ecosystem. In 2017, initial coin offerings would explode, raising a collective $5.1 billion. All of this was done without a single registration being filed with the SEC, and many of these initial coin offerings—including

---

* Assistant Professor of Law, The John Marshall Law School. I would like to thank Mitchol Dunham for his extensive research assistance without which this article would not have been possible. I would also like to extend my heartfelt thanks to my colleagues at the University of Denver Sturm College of Law for their invaluable feedback and advice in preparing this article.

several $100 million raises—were based on little more than a white paper and a few lines of sample code. Welcome to the new Digital Wild West.

With the seemingly overnight success of this new funding mechanism, there is little legal scholarship addressing initial coin offerings and how, or if, such offerings should be regulated. This Article provides a non-technical legal audience with a foundational understanding of how the blockchain works and the role initial coin offerings play in this new economic ecosystem. The overarching thesis of the article is that our current securities law framework, a framework that dates to the days of the Great Depression, is ill-equipped to handle this new world of decentralized, global, pseudonymous fund raises on public blockchains. Instead, governmental regulators should be working with core development teams to build a regulatory framework that integrates investor protections directly into the computer code governing these systems. By embracing "code as law," both regulators and core development teams can protect the innovation being funded by initial coin offerings, while at the same time injecting some much-needed investor protections into this new ecosystem.

This Article begins with an introduction to the coming decentralized world, including an overview of both public blockchain technology as well the Ethereum platform, the primary public blockchain upon which initial coin offerings are being deployed. Central to this introduction is an explanation of how the decentralization and disintermediation brought by the blockchain has the potential to dramatically reshape our economic and social systems. Next, the Article explores the recent explosion of initial coin offerings, discussing how these offerings are structured, and how this new funding mechanism, if developed properly, has the promise of democratizing opportunities for economic innovation. The Article then examines the SEC's early statements on initial coin offerings to illustrate the potential problems with applying a dated legal framework to this new technology. Finally, the Article concludes that the traditional securities law framework is ill-suited for the coming decentralized world because the SEC's enforcement power over global blockchain platforms is limited. Recognizing that external legal frameworks cannot be forced upon public blockchain platforms, the Article argues for a collaborative process where governmental regulators work with core development teams to build a regulatory framework into the very fabric of these platforms, thereby providing investors protection, while at the same time embracing the concept of code as law.

INTRODUCTION

In the spring of 2016 a new type of entity called The DAO—short for decentralized autonomous organization—became one of the most successful crowdfunded entities in history, raising over $150 million in less than thirty days.[1] Despite this massive fund raise, The DAO was not registered as a legal entity in any sovereign jurisdiction.[2] Nor did The DAO have a board of directors, a CEO, or a management team.[3] Moreover, because it was not a legally recognizable corporate entity and because it was funded through cryptocurrencies that made it difficult to determine the origin of the funds, it is unclear if or how a court could assert jurisdiction over The DAO or its members in the case of a dispute.[4] Formed as a decentralized venture capital fund, The DAO's sole purpose was to fund the development of new software

---

1. *See* Dino Mark, Vlad Zamfir & Emin Gün Sirer, *A Call for a Temporary Moratorium on The DAO*, HACKING, DISTRIBUTED (May 27, 2016, 1:35 PM), http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/.

2. *See* CHRISTOPH JENTZSCH, DECENTRALIZED AUTONOMOUS ORGANIZATION TO AUTOMATE GOVERNANCE 1–2 [hereinafter JENTZSCH WHITE PAPER], https://download.slock.it/public/DAO/WhitePaper.pdf (describing basic structure of decentralized autonomous organizations); *see also* Christoph Jentzsch, *The History of The DAO and Lessons Learned*, MEDIUM: SLOCK.IT BLOG (Aug. 24, 2016) [hereinafter *The History of The DAO*], https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5 ("We wanted to go even further and create a 'true' DAO one that would be the *only and direct* recipient of the funds, and would represent the creation of an organization similar to a company, with potentially thousands of Founders.").

3. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 1–2; *The History of the DAO and Lessons Learned*, *supra* note 2.

4. Andrew Hinkes, *The Law of The DAO*, COINDESK (May 19, 2016, 16:15 UTC), https://www.coindesk.com/the-law-of-the-dao/ ("It is unclear whether the actions of a DAO would be attributed to the creators of that DAO, those who maintain that DAO, those who suggest projects, or those who have invested in a DAO. . . . If a lawsuit were filed against a DAO, it would stall immediately because of the difficulty of identifying a party who represents the DAO to serve with process."); *see also* ALLEN & OVERY LLP, DECENTRALIZED AUTONOMOUS ORGANIZATIONS 5–6 (2016), http://www.allenovery.com/SiteCollectionDocuments/Article%20Decentralized%20Autonomous%20Organizations.pdf ("DAOs are not currently recognized legal entities, creating uncertainty as to the legal rights attributable to a DAO and who bears the legal responsibilities. . . . While a DAO might have extensive rules governing its conduct between internal members, those rules may be of little use when interacting with an external jurisdiction's legal system."); Jeffrey K. Berns, *Understanding Ethereum and The DAO Conundrum*, BERNS WEISS LLP (July 5, 2016, 5:28 PM), https://www.law111.com/understanding-ethereum-and-the-dao-conundrum ("[T]here is no way to identify The DAO in a way that has legal significance or to identify anyone with the authority to represent The DAO's interest in a lawsuit.").

applications.[5] But before The DAO was fully operational, it was hit with a cyber-attack that drained over one-third of its funds and put an early end to this ambitious experiment.[6] Although The DAO is no longer operational, its completely unregulated nine-figure fund raise has given rise to widespread adoption of one of the most efficient yet controversial corporate funding mechanisms in history—the initial coin offering or "ICO."

In addition to The DAO, in 2016, sixty-four separate entities conducted ICOs (also known as token sales or issuances), collectively raising $103 million.[7] Those numbers would explode in 2017, with ICOs collectively raising an estimated $5.1 billion.[8] In late May 2017, Brave, a company developing a decentralized web browser, raised an astonishing $35 million in less than 30 seconds.[9] That is not a typo—$35 million in 30 seconds.[10] Not to be outdone, in June 2017, Block.one, a company building an enterprise blockchain platform, raised $185 million over just five days.[11] Shortly thereafter, Bancor, a company developing a cryptocurrency exchange platform, raised in excess of $153 million in just three hours.[12] Brave, Block.one, and Bancor are just the tip of the iceberg, with new ICOs launching almost

---

5. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2.

6. *The History of The DAO*, *supra* note 2 ("On the 17th of June, the attacker withdrew around 3.5M ETH (~50M$) from the DAO . . . ."). Importantly, The DAO was not hacked or compromised. Instead, a hacker or hackers exploited a flaw in the code governing the system, which allowed siphoning off of funds from The DAO. *Id.*

7 Connie Loizos, *How to Stage an ICO (and Answers to Other Lingering Questions You Might Have)*, TECHCRUNCH (May 24, 2017), https://techcrunch.com/2017/05/24/how-to-stage-an-ico-and-other-related-questions-you-might-like-answered/.

8. *See* SHERWIN DOWLAT, CRYPTOASSET MARKET COVERAGE INITIATION: NETWORK CREATION 20 (July 11, 2018), https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ.

9. *See* Jon Russell, *Former Mozilla CEO Raises $35M in Under 30 Seconds for His Browser Startup Brave*, TECHCRUNCH (June 1, 2017), https://techcrunch.com/2017/06/01/brave-ico-35-million-30-seconds-brendan-eich/.

10. *See id.*

11. *See* Mo Marshall, *$185 Million in 5 Days: Block.one Sets New ICO Record with Its EOS Token*, VENTUREBEAT (July 1, 2017, 12:44 PM), https://venturebeat.com/2017/07/01/185-million-in-5-days-block-one-sets-new-ico-record-with-its-eos-token/.

12. *See* Stan Higgins, Alex Sunnarborg & Pete Rizzo, *$150 Million: Tim Draper-Backed Bancor Completes Largest-Ever ICO*, COINDESK (June 12, 2017, 13:30 UTC), https://www.coindesk.com/150-million-tim-draper-backed-bancor-completes-largest-ever-ico/; Stan Schroeder, *This Startup Used Ethereum to Raise $150 Million in Three Hours*, MASHABLE (June 13, 2017), http://mashable.com/2017/06/13/bancor-ico-ethereum/#0ssxy_0c35q8.

daily.[13] Unlike The DAO, the majority of these entities are structured as traditional companies,[14] but many of these fund raises were done completely free from government regulation and without complying with United States or other securities laws.[15] So how did these companies raise such extraordinary amounts without attracting the attention of securities regulators? Simple, these fund raises occurred not in the physical world but on Ethereum, a public blockchain platform.[16] Welcome to the new Digital Wild West.

With the explosion of both the number of ICOs and the steep increase in the funds being raised, many both within and outside the blockchain space began questioning whether governmental regulators

---

13. *See* Jen Wieczner, *Cryptocurrency ICOs Are Making Bitcoin Startups Richer than VCs Ever Did*, FORTUNE (July 28, 2017), http://fortune.com/2017/07/28/bitcoin-cryptocurrency-ico/; *see also* Laura Shin, *The Emperor's New Coins: How Initial Coin Offerings Fueled a $100 Billion Crypto Bubble*, FORBES (July 27, 2017), https://www.forbes.com/sites/laurashin/2017/07/10/the-emperors-new-coins-how-initial-coin-offerings-fueled-a-100-billion-crypto-bubble/#19badad36ece (discussing numerous other ICOs and adding, "[t]hese initial coin offerings have raised more than $850 million").

14. *See* Loizos, *supra* note 7 (stating that ICOs are a "global industry" including companies "in the U.S. and structured through Delaware" and foreign companies "structured in Switzerland [and] some in Singapore"). There are some ICOs that have launched without the founders ever forming a legal entity. *See* Shin, *supra* note 13 ("The entities raising money in these coin offerings are not always startups. Sometimes they're merely developers collaborating on a project and don't form a legal entity.").

15. David Zeiler, *Why Initial Coin Offerings (ICOs) Raise Millions of Dollars in Seconds*, WALL STREET EXAMINER (June 6, 2017), http://wallstreetexaminer.com/2017/06/initial-coin-offerings-icos-raise-millions-dollars-seconds/ ("Frankly, it's not clear whether ICOs are even legal under current law. While crowdfunding for startups was made legal by the JOBS Act, a number of restrictions apply. And ICOs appear to violate several of them."); *see also* Shin, *supra* note 13 ("[E]ven when the group is really a corporation, such as the messaging app Kik, which is launching the Kin token, the organizers will claim that the crowdsale is not actually offering a share of the company, conveniently sidestepping securities regulations.").

16. Ethereum is not the only blockchain platform giving rise to ICOs. In fact, as of the writing of this Article in October 2017, the most successful ICO of all time belongs to Tezos, whose July 2017 ICO raised in excess of $230 million. *See* Anna Irrera, Steve Stecklow & Brenna Hughes Neghaiwi, *Special Report—Backroom Battle Imperils $230 Million Cryptocurrency Venture*, REUTERS (Oct. 18, 2017, 6:02 PM), https://www.reuters.com/article/bitcoin-funding-tezos/special-report-backroom-battle-imperils-230-million-cryptocurrency-venture-idUSL4N1MT53I. Tezos does not run on the Ethereum platform but instead is its own independent public blockchain platform. *Id.*

would continue to sit on the sidelines.[17] In July 2017, the United States Securities and Exchange Commission answered that question when it issued a report detailing the findings of its investigation into The DAO.[18] In its report, the SEC concluded that DAO tokens are securities under the seventy-year-old *Howey* test.[19] In the year since the SEC issued its report, it has brought numerous enforcement actions against token issuers and issued numerous consumer fraud alerts and other warnings related to ICOs.[20] So after months of speculation and billions of dollars raised without any supervision, the SEC has now planted its regulatory flag.[21] Finally, U.S. investors and blockchain entrepreneurs have an answer: ICOs are subject to federal securities laws—well, maybe.[22]

The SEC's conclusion that DAO tokens are securities ignores critical facts and reaches a conclusion that does not square with existing case law. Interestingly, the SEC's report contains no discussion or analysis regarding common enterprise, one of the three *Howey* requirements. Nor does it provide an accurate factual picture of the operation of The DAO in support of its conclusion as to another *Howey* requirement—that DAO token holders relied on the efforts of others. After reaching the conclusion that DAO tokens are securities,[23] the SEC nonetheless states that it has no intention of

---

17. *See, e.g.*, Camila Russo, *Ethereum Co-Founder Says Crypto Coin Market Is a Time-Bomb*, BLOOMBERG (July 18, 2017, 1:40 PM), https://www.bloomberg.com/news/articles/2017-07-18/ethereum-co-founder-says-crypto-coin-market-is-ticking-time-bomb ("Regulation is the biggest risk to the sector, as it's likely that the U.S. Securities and Exchange Commission, which has remained on the sidelines, will step in to say that digital coins are securities . . . .").

18. U.S. SEC. & EXCH. COMM'N, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO (2017) [hereinafter SEC REPORT], https://www.sec.gov/litigation/investreport/34-81207.pdf. That same day, the SEC also released an Investor Bulletin warning the public of the potential for fraud in the ICO marketplace. *See Investor Bulletin: Initial Coin Offerings*, U.S. SEC. & EXCH. COMM'N (July 25, 2017), https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

19. SEC REPORT, *supra* note 18, at 11–18; *see also* SEC v. W.J. Howey Co., 328 U.S. 293, 299 (1946).

20. *See infra* Section IV.B.

21. *See generally* SEC REPORT, *supra* note 18.

22. *See id.* at 17–18 ("Whether or not a particular transaction involves the offer and sale of a security—regardless of the terminology used—will depend on the facts and circumstances, including the economic realities of the transaction.").

23. *Id.* at 1 ("Based on the investigation, and under the facts presented, the Commission has determined that DAO Tokens are securities under the Securities Act of 1933 . . . and the Securities Exchange Act of 1934 . . . ."). Other sovereign governments were quick to follow the United States. In September 2017, China

pursuing an enforcement action against The DAO.[24] So while the report gives insight into the SEC's view of one specific ICO, both the report's legal conclusions and the general applicability of those conclusions to other ICO structures are, at best, questionable. In addition to the problematic analysis itself, the SEC's report rushed past a critical threshold question: are the traditional rules governing securities offerings, rules established in the early part of the last century, the best legal framework to regulate this new technology-driven funding mechanism? Unfortunately, the SEC's early enforcement actions, fraud alerts, and other statements have failed to address this critical question.

Currently, there is little legal scholarship discussing the blockchain and virtually none addressing initial coin offerings. As such, this Article provides a non-technical legal audience with a foundational understanding of how the blockchain works and the role ICOs play in this new economic ecosystem. In Part I, I provide an introduction to the coming decentralized world, including an overview of both public blockchain technology as well the Ethereum platform, the primary public blockchain upon which ICOs are being deployed.[25] In Part II, I explore the recent explosion of ICOs, discussing how these offerings are structured, and how this new funding mechanism, if developed properly, will democratize opportunities for economic innovation. In Part III, I turn to the SEC's report on The DAO and its conclusion that DAO tokens are securities. Through a detailed examination of both the SEC's report and the operations of The DAO, as well as a brief overview of the SEC's early enforcement actions in

---

announced a complete ban on ICOs. *See* Jon Russell, *First China, Now South Korea Has Banned ICOs*, TECHCRUNCH (Sept. 28, 2017), https://techcrunch.com/2017/09/28/south-korea-has-banned-icos/.

24. SEC REPORT, *supra* note 18, at 1 ("The Commission has determined not to pursue an enforcement action in this matter based on the conduct and activities known to the Commission at this time.").

25. Public blockchains are sometimes referred to by other names, including distributed public ledgers or decentralized public ledgers. The blockchain is just one type of distributed public ledger, and other variations of distributed public ledgers may operate in slightly different ways. An analogy to Band-Aids might be helpful. While Band-Aid is a name brand for first aid supplies, it is also frequently used to identify this general category of first aid supplies regardless of the manufacturing company. Similarly, the term "blockchain" originated with Bitcoin but is now widely used as short hand for many similar distributed public ledgers. In this Article, I use the phrase "the blockchain" to generally describe public blockchains, including the Bitcoin and Ethereum Blockchains. It is also important to note that while there is significant work being done by private companies to develop closed or private blockchains, the focus of this Article is solely on public blockchains.

the blockchain space, I conclude that the SEC's analysis is flawed, both regarding its finding of a "common enterprise" and its conclusion that DAO token holders' expectation of profits were dependent on the "efforts of others."

Finally, in Part IV, I discuss the fallout and potential long-term implications of the SEC's early foray into ICO regulation. Ultimately, I conclude that the traditional securities law framework is ill-suited for the coming decentralized world, that a heavy-handed regulatory crackdown will lead to the loss of both innovation and capital investment opportunities, and that while it is actively asserting itself in the ICO space, the SEC will face considerable challenges to enforcing U.S. securities laws in the global blockchain ecosystem. I will explain why external legal frameworks should not be forced upon public blockchain platforms but instead must develop through a collaborative process where governmental regulators work with core development teams. Through such a process, a regulatory framework could be built into the very fabric of these platforms, thereby providing investors protection, while at the same time embracing the concept of code as law.[26]

I. OVERVIEW OF DECENTRALIZED LEDGER SYSTEMS

It is likely that if you are reading this Article you are either an attorney or legal academic who is curious about the recent explosion of bitcoin and cryptocurrency headlines. You likely picked up this Article to better understand the legal issues accompanying this new and burgeoning world of blockchains, tokens, and the suddenly ubiquitous multi-million dollar fund raises that seemingly emerged from nowhere overnight. You came to a legal journal in order to avoid a long trip through the technical jargon and conceptual complexity inherent in any discussion of the blockchain. Well, I am sorry to

---

26. The concept of code as law—the idea that computer code does or should provide the legal and regulatory frameworks governing activity within software systems—has been written about extensively by Professor Lawrence Lessig, among others. *See, e.g.*, Lawrence Lessig, *Code Is Law: On Liberty in Cyberspace*, HARV. MAG. (Jan. 1, 2000), https://harvardmagazine.com/2000/01/code-is-law-html ("This regulator is code—the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates.").

inform you, but I must begin with a disclaimer: in order to understand what ICOs are, how they work, and where they fit into the current regulatory environment, you must first have a working understanding of the blockchain and cryptocurrencies. You need not be a software developer or master cryptographer, but understanding the operation and potential impacts of this new technology is essential because the underlying concepts—decentralization and disintermediation—promise to challenge many commonly-held conceptions about what is and is not possible in the world, what has and does not have value, and how we, as a society, build consensus amongst ourselves. That said, I recommend that you lean into this new world and embrace the challenge of a short, albeit interesting trip down the blockchain rabbit hole.

A. Big Picture: The Shift to a Decentralized World

Over the last decade, numerous technology-driven companies have emerged and "disrupted" traditional markets—or so we are told. Uber "disrupted" the transportation industry,[27] Airbnb "disrupted" travel and lodging,[28] and Netflix "disrupted" cable television and media.[29] These companies may have disrupted their respective industries by pioneering new ways of aggregating and then exploiting supply and demand, but they did not fundamentally change the well-established centralized control model.[30] While it is George the college student who you summon for a ride through an app on your phone, it is Uber, a multi-national company with a $69 billion market cap, to which you pay your fare.[31] So yes, Uber has replaced Yellow Taxis and Airbnb may have replaced Marriott, but replacing one large

---

27. *See* Emily Isaac, *Disruptive Innovation: Risk-Shifting and Precarity in the Age of Uber* 2 (Berkeley Roundtable on the Int'l Econ., Working Paper No. 2014-7, 2014), http://www.brie.berkeley.edu/wp-content/uploads/2015/01/Disruptive-Innovation.pdf.

28. Jeroen Oskam & Albert Boswijk, *Airbnb: The Future of Networked Hospitality Businesses*, 2 J. TOURISM FUTURES 22, 22 (2016).

29. *See* Larry Downes & Paul Nunes, *Big-Bang Disruption*, HARV. BUS. REV. Mar. 2013, at 44, 48.

30. *See* DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD 17 (2016).

31. *See id.* ("But these businesses have little to do with sharing. In fact, they are successful precisely because they do not share—they aggregate."); *see also* Leila Abboud, *Uber's $69 Billion Dilemma*, BLOOMBERG (Mar. 16, 2017, 4:30 AM), https://www.bloomberg.com/gadfly/articles/2017-03-16/uber-needs-to-get-real-about-that-69-billion-price-tag (setting Uber's market cap at $69 billion as of March 2017).

corporation with another is less disruption than simple market evolution. The blockchain represents a move to a new relational paradigm, one that shifts the focus from centralized institutions to peer-to-peer transactions between individual participants in the market place. This democratization of commerce has the potential to be, for lack of a better term, truly disruptive.

This is not the first time that futurists have declared that a new technology would topple the centralized power structures that dominate our economic and social systems.[32] Many early observers of the internet believed that the World Wide Web held this promise.[33] In *Blockchain Revolution*, noted technologists Don and Alex Tapscott use a helpful Star Wars analogy to describe the unfulfilled promise of the Internet:

> The first era of the Internet started with the energy and spirit of a young Luke Skywalker—with the belief that any kid from a harsh desert planet could bring down an evil empire and start a new civilization by launching a dot-com. Naïve to be sure, but many people, present company included, hoped the Internet, as embodied in the World Wide Web, would disrupt the industrial world where power was gripped by the few and power structures were hard to climb and harder to topple. . . . Low cost and massive peer-to-peer communication on the Internet would help undermine traditional hierarchies and help with the inclusion of developing world citizens in the global economy. . . . The world would be flatter, more meritocratic, more flexible, and more fluid. . . . Some of this has come to pass. . . . However, the Empire struck back. It has become clear that concentrated powers in business and government have bent the original democratic architecture of the Internet to their will.[34]

So what is different this time? The idea of the blockchain emerged during a time of crumbling faith in the centralized institutions that dominate our current world—namely large financial institutions, central banks, and sovereign governments.[35] Proposed at the height of the 2008 global financial crisis, the blockchain was conceived of and

---

32. *See* TAPSCOTT & TAPSCOTT, *supra* note 30, at 12.

33. *Id.*

34. *Id.*

35. *See* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008) [hereinafter BITCOIN WHITE PAPER], https://bitcoin.org/bitcoin.pdf.

built around a paradigm of decentralized consensus as opposed to centralized control.[36] The peer-to-peer architecture of the technology itself, as well as its open source accessibility and privacy ensured through encryption, allows for the direct exchange of value between parties without interference from banks, governments, or other intermediaries.[37]

It is difficult to overstate the change afoot in moving from a centralized to a decentralized world. While few take time to think about it, our entire world is shaped by dominance of centralized institutions.[38] These institutions dictate what has value, what we individually earn, what we can and cannot purchase, and ultimately who has and does not have power in our economic system. This rigid hierarchal structure has largely governed economic, political, and social systems in the post-World War II world.[39] World affairs are controlled by central governments; the global economy is dominated by large corporations and financial institutions with centralized management structures; and our day-to-day interactions, including banking, shopping, and even earning a living from our labor, are largely dependent on centralized intermediaries. The blockchain has the potential to change much of that. It presents a new way for us as individuals to trade value and reach consensus, and thus, it presents an opportunity to remake our economic, social, and governmental systems to better serve the best interest of all people instead of a select few who control the current corporate and political hegemonies. And while the increased democratization promised by this decentralization is not a foregone conclusion, the potential for this change has perhaps never been greater.

---

36. *See generally id.*

37. *See generally id.*

38. *See* TAPSCOTT & TAPSCOTT, *supra* note 30, at 17–20 (discussing the role of centralized institutions).

39. *See* NATASHA EZROW, GLOBAL POLITICS AND VIOLENT NON-STATE ACTORS 11 (2017) ("The heavy focus on the state materialized in the post-World War II era . . . .").

B. What Is the Blockchain?

Chances are good that you are familiar with the cryptocurrency bitcoin, and perhaps you have read an article or two on the blockchain and its loudly trumpeted promise of changing the world.[40] Despite the many media and academic articles that have propelled bitcoin from fringe tech-circles to mainstream,[41] there is still little understanding amongst the public as to how cryptocurrencies work and even less understanding as to the technology that underpins these currencies—the blockchain. This is not an article about bitcoin, but to understand the power of public blockchains and the burgeoning decentralized world, including the explosion of ICOs, one has to start at the beginning, and it all began with bitcoin.

In 2008, a person or persons working under the pseudonym Satoshi Nakamoto published a white paper introducing the world to bitcoin, a cryptocurrency system that is neither produced nor regulated by any sovereign government.[42] The white paper contemplated "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[43] In less than a decade, bitcoin has moved from the underground

---

40. *See, e.g.*, Bernard Marr, *How Blockchain Technology Could Change the World*, FORBES (May 27, 2016, 2:46 AM), https://www.forbes.com/sites/bernardmarr/2016/05/27/how-blockchain-technology-could-change-the-world/#3f84c0cd725b; Rob Marvin, *Blockchain: The Invisible Technology That's Changing the World*, PC MAG (Aug. 29, 2017, 1:38 PM), https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor; Alex Tapscott & Don Tapscott, *Here's Why Blockchains Will Change the World*, FORTUNE (May 8, 2016), http://fortune.com/2016/05/08/why-blockchains-will-change-the-world/.

41. *See, e.g.*, Suzanne McGee, *Why You Should Care About Bitcoin: Digital Currency Is Here to Stay*, GUARDIAN (Apr. 9, 2014, 11:55 AM), https://www.theguardian.com/money/us-money-blog/2014/apr/09/why-bitcoins-matter-digital-currency-future; Rob Price, *Weed, Times Square, and Floyd Mayweather: How Cryptocurrency Mania Is Creeping into the Mainstream*, BUS. INSIDER (Sept. 1, 2017, 9:28 AM), http://www.businessinsider.com/cryptocurrency-bitcoin-ethereum-ico-mania-going-mainstream-2017-8; Peter Tchir, *Bitcoin Is Going Mainstream*, FORBES (Aug. 2, 2017, 9:42 AM), https://www.forbes.com/sites/petertchir/2017/08/02/bitcoin-is-going-mainstream/#123a3d053c9c.

42. *See* BITCOIN WHITE PAPER, *supra* note 35, at 1.

43. *Id.*; *see also* Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ L. REV. 359, 412 (2016) ("[I]ndeed the purpose of Bitcoin was to offer a peer-to-peer alternative to the trusted intermediary approach.").

cypherpunk community[44] to a globally significant currency with a market cap in excess of $200 billion as of January 2018.[45] While the evolution and growth of bitcoin poses new and challenging legal questions, the academic and media obsession with the cryptocurrency has obscured the true innovation—the blockchain.[46]

The blockchain is a distributed public ledger that uses a mathematical consensus protocol to allow the exchange of value between two parties who otherwise do not know or trust one another.[47] This "trustless-trust" transfer allows strangers to exchange value of any sort without the need for banks, escrow agents, attorneys, accountants, and other intermediaries.[48] In the simplest terms, the blockchain is a ledger that can be used to record virtually any type of transaction: transfers of cryptocurrency, medical records, real estate chains of title, and everything in between.[49] So how does this new technology differ from our current value exchange systems, and how can anyone have confidence in a currency that has neither a physical

---

44. *See* Eric Hughes, *A Cypherpunk's Manifesto*, ACTIVISM.NET (Mar. 9, 1993), https://www.activism.net/cypherpunk/manifesto.html ("We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.").

45. Market Cap for Bitcoin as of January 2018, COINMARKETCAP, https://coinmarketcap.com/currencies/bitcoin/ (follow "Historical Data" hyperlink; then search date range for "All Time" and scroll down to Jan. 2018).

46. See Joshua A.T. Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805, 808–09 (2015) ("Most of the discussion in the legal literature and the news media to date has centered around the use of such public ledgers as a substitute for currency. However, a distributed public ledger system confers not just the power to transfer dollars, but also the power to transfer anything. . .'The breakthrough means that, theoretically, any act of commerce on the Web can be decentralized and stripped of controlling authority.'" (quoting Rob Wile, *Satoshi's Revolution: How the Creator of Bitcoin May Have Stumbled onto Something Much, Much Bigger*, BUS. INSIDER (Apr. 22, 2014, 11:50 AM), https://www.businessinsider.com/the-future-of-the-blockchain-2014-4)).

47. *See* BITCOIN WHITE PAPER, *supra* note 35, at 3.

48. *See* Edward D. Baker, *Trustless Property Systems and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange*, 45 SW. L. REV. 351, 357–58 (2015) ("While a traditional digital property system, such as PayPal, acts as a trusted third party that moderates and completes a transaction, TPL technology removes the middleman, and enables users to exchange digital property securely and anonymously over the network without any prior relationship.").

49. *See id.* at 357 ("In simple terms, a Trustless Public Ledger is a public list describing the chain of ownership of a given piece of property or something of value."); Bernard Marr, *A Complete Beginner's Guide to Blockchain*, FORBES (Jan. 24, 2017, 12:37 AM), https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/2/#54dee30560ec.

form nor backing from a government or central bank? The answer is that the blockchain is set-up as a peer-to-peer network that allows its participants to agree on the state of the ledger at any given time by reaching consensus through a mathematical protocol.[50] Because individual participants work together to ensure that the blockchain is accurate and secure, it is not dependent on the actions of any single central authority.[51]

In the 2008 white paper, Nakamoto laid the groundwork for the coming decentralized world by providing a solution to the so-called "double-spend" problem, a problem that until that time had prevented widespread use of digital currencies.[52] The double-spend problem is relatively straight forward: digital currency is nothing more than a computer file, so how do you prevent one party from spending or transferring the same digital coin multiple times?[53] In our existing economic system, this problem is solved by central governments that mint and control the currency supply through central banks.[54] In contrast, Nakamoto's white paper presented a new way for humans to reach consensus on the state of reality—that is, agreement between participants on what transactions had and had not occurred, and in what order those transactions occurred, through a mathematical consensus protocol that does not require a trusted central authority.[55]

---

50. *See* Baker, *supra* note 48, at 358 (citing BITCOIN WHITE PAPER, *supra* note 35) ("TPLs deploy a system of cryptographic proofs to secure each transaction.").

51. *See id.* (citing Paul Farmer, *Speculative Tech: The Bitcoin Legal Quagmire and the Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85, 88–89 (2014)).

52. *See* BITCOIN WHITE PAPER, *supra* note 35, at 1. Bitcoin was not the first time "cypherpunks" attempted to solve the double-spend problem through cryptography. The eventual basis of Bitcoin's proof-of-work system was suggested well over a decade earlier as a means of battling junk e-mail. *See* CYNTHIA DWORK & MONI NAOR, PRICING VIA PROCESSING OR COMBATTING JUNK MAIL 1 (1992), http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf. The concepts proposed in Dwork and Naor's article were applied in a financial context in 1997 through a system called Hashcash. Posting of Adam Back, aba@dcs.ex.ac.uk, to owner-cypherbunks@toad.com (Mar. 28, 1997) (on file with author). Following Hashcash, several other proof-of-work based cash systems were created, such as b-money and e-gold in the late 1990s, but cryptocurrencies did not see widespread success until the creation of Bitcoin in 2008. *See* SARAH JEONG, THE BITCOIN PROTOCOL AS LAW, AND THE POLITICS OF A STATELESS CURRENCY 11 (2013) (describing the iterations of cryptocurrencies through the 1990s and culminating with Bitcoin).

53. *See* BITCOIN WHITE PAPER, *supra* note 35, at 2; *see also* Jacob Hamburger, Note, *Bitcoins vs. State Money Transmission Laws: Protecting Consumers or Hindering Innovation?*, 11 J.L. ECON. & POL'Y 229, 232 (2015).

54. *See* BITCOIN WHITE PAPER, *supra* note 35, at 2.

55. *See id.*

To see how this is a game changer, let's look at a simple example: Party A utilizes a credit card to purchase widgets from Party B. There is no physical transfer of money; instead, the process is handled by central authorities. Once Party A swipes the card, Party B's card processing system sends the card data to an acquirer bank (also known as a payment processor).[56] The acquirer bank then sends the data to the payment brand—Visa, MasterCard, American Express, etc.—who then forwards the data to the bank that issued the card.[57] The issuing bank verifies the legitimacy and validity of the card (that it is not stolen, has funds available, etc.).[58] Once verified, the issuing bank generates an authorization number and routes this number back to the card brand.[59] The card brand then forwards the authorization code back to the acquirer bank, which then sends the code back to the Party B.[60] Once Party B has an authorization code, it completes the transaction.[61] Thus, a simple payment includes at least three centralized intermediaries: the acquirer bank, the payment brand, and the issuing bank.[62] Each of these entities has overhead, and each therefore charges a small transaction fee on every transaction.[63] In the traditional banking and credit system there is no way to avoid these fees—if you are going to move money, you must pay the toll.

C. How the Blockchain Works

In contrast to the above example, the blockchain allows a direct and secure transfer of value from Party A to Party B.[64] Public blockchains have five characteristics that make this secure peer-to-peer value exchange possible: (1) blockchains are distributed—via a peer-to-peer network with no central server; (2) blockchains are accessible—operating on an open source software that anyone can run for free; (3) blockchains are transparent—all transactions on the

---

56. *See* FIRST DATA, PAYMENTS 101: CREDIT AND DEBIT CARD PAYMENTS, KEY CONCEPTS AND INDUSTRY ISSUES 7 (2010), https://www.firstdata.com/downloads/thought-leadership/payments101wp.pdf.

57. *See id.*

58. *See id.*

59. *See id.*

60. *See id.*

61. *See id.*

62. *See id.* at 8.

63. *See* Amad Ebrahimi, *The Complete Guide to Credit Card Processing Rates & Fees*, MERCHANT MAVERICK (Aug. 23, 2018), https://www.merchantmaverick.com/the-complete-guide-to-credit-card-processing-rates-and-fees/.

64. *See* Baker, *supra* note 48, at 358.

blockchain can be seen by all participants on the network; (4) blockchains are permanent and largely immutable—once validated, it is nearly impossible for a transaction to be altered or deleted;[65] and (5) blockchains are secure—encrypted and largely impervious to outside attack.[66]

---

65. *See* BITCOIN WHITE PAPER, *supra* note 35, at 2–6.

66. While difficult and impractical, it is possible to alter or delete transactions through a 51% attack, a Sybil attack, or a hard fork. A 51% attack harnesses the computing power of 51% of the nodes on the network to transmit false information. On the blockchain, the "true" version of events correlates with the longest chain, as determined by more than 50% agreement amongst nodes as to the validity of a block. Once the nodes breach 50% agreement on a block's validity, it is added to the chain, and the subsequent block will be added to this block. Thus, if 51% of the network is controlled by a bad actor, that bad actor could theoretically double spend funds out of his or her account by spending more than once from a single account in different blocks. By controlling 51% of nodes on the network, the bad actor could validate the double-spend transactions without debiting his or her account. While a 51% attack is the technical name for this type of attack, it could be done with a much lower percentage of the computing power and some luck. On the other hand, 51% guarantees that the attack will be successful in the long term. *See, e.g.*, MARTIJN BASTIAAN, PREVENTING THE 51%-ATTACK: A STOCHASTIC ANALYSIS OF TWO PHASE PROOF OF WORK IN BITCOIN 2 (2015), http://fmt.cs.utwente.nl/files/sprojects/268.pdf; Kyle Torpey, *Why a 51% Attack Is Not What Most Bitcoin Users Think It Is*, COINJOURNAL (Sept. 7, 2015) (quoting SF Bitcoin Developers, *SF Bitcoin Devs Seminar a Special Presentation by Matt Corallo of Blockstream*, YOUTUBE (Aug. 17, 2015), https://www.youtube.com/watch?v=XEiVbkeZjuQ), https://coinjournal.net/why -a-51-attack-is-not-what-most-bitcoin-users-think-it-is/; *see also infra* note 113 and accompanying text.

A Sybil, or pseudospoofing, attack occurs when a bad actor creates fake nodes that broadcast only the bad actor's interpretation of the consensus such that only the bad actor's blocks are validated. This attack can largely be mitigated through the imposition of proportional computational requirements to the creation of the block; however, combined with a 51% attack, it is an effective method of chain manipulation. *See, e.g.*, John R. Douceur, *The Sybil Attack*, *in* PEER-TO-PEER SYSTEMS 251–60 (Peter Druschel, Frans Kaashoek & Antony Rowstron eds., 2002); Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski & Lukasz Mazurek, *Secure Multiparty Computations on Bitcoin*, 2014 IEEE SYMP. ON SEC. & PRIVACY 444, 447 (2014), http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6956580; Alex Biryukov & Ivan Pustogarov, *Bitcoin over Tor Isn't a Good Idea*, 2015 IEEE SYMP. ON SEC. & PRIVACY 122, 129 (2015), http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7163022.

A hard fork is a change in the code of a software system that makes the new code incompatible with the older code. In contrast, a soft fork maintains backwards compatibility with the previous code. Both Bitcoin and Ethereum have implemented hard forks that, among other changes, altered the size of blocks and redistributed funds "stolen" from The DAO to their rightful owners. This latter example of hard forking is what creates the ability to change or alter transactions despite the transactions being validated and added to the chain. *See, e.g.*, SERGEI TIKHOMIROV,

Instead of being housed in a singular location (a central server for example), information on the blockchain exists simultaneously on every computer (or nodes as they are known in the blockchain world) on the network.[67] By distributing the ledger across hundreds, thousands, or even millions of nodes, public blockchains ensure that there is no single point of failure in the system that could be attacked or exploited by bad actors.[68] Public blockchains are built on open source software that can be accessed by anyone with a computer and an internet connection.[69] This low barrier to entry and open-source accessibility allows for increased participation (all you have to do is download the client software), which leads to the democratization (or at least the potential of democratization) of business, social, and governance systems that run on the blockchain.[70]

Next, public blockchains are transparent and secure.[71] Every transaction that is recorded to the blockchain can be seen by every node on the network.[72] Because everyone on the network can see every transaction, it is difficult for a single bad actor to unilaterally post fraudulent transactions.[73] Transactions on the blockchain are secured through two cryptographic devices: public-private key encryption and hash functions.[74] Public-private keys allow for value to be sent to anyone who wishes to participate on the blockchain and ensure that

---

ETHEREUM: STATE OF KNOWLEDGE AND RESEARCH PERSPECTIVES 5 n.4, 9–10 (2017), http://orbilu.uni.lu/bitstream/10993/32468/1/ethereum-sok.pdf; Vitalik Buterin, *Hard Fork Completed*, ETHEREUM BLOG (July 20, 2016), https://blog.ethereum.org/2016/07/20/hard-fork-completed/; Alyssa Hertig, *Hard Forks Galore: Bitcoin Cash Debates Ambitious Tech Roadmap*, COINDESK (Aug. 30, 2017), https://www.coindesk.com/hard-forks-galore-bitcoin-cash-debates-ambitious-tech-roadmap/; Antonio Madeira, *The DAO, the Hack, the Soft Fork and the Hard Fork*, CRYPTOCOMPARE (July 26, 2016), https://www.cryptocompare.com/coins/ guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/.

67. *See* BITCOIN WHITE PAPER, *supra* note 35, at 3.

68. *See id.* at 1, 3–8.

69. *See id.* at 3–4.

70. *See id.* at 2–3.

71. *Id.* at 3.

72. *Id.* at 2–3.

73. *See* Nick Vogel, *The Great Decentralization: How Web 3.0 Will Weaken Copyrights*, 15 J. MARSHALL REV. INTELL. PROP. L. 136, 139 (2015) (citing Larry Greenenmeier, *Bitcoin-Based Blockchain Breaks Out*, SCI. AM. (Apr. 1, 2015), https://www.scientificamerican.com/article/bitcoin-based-blockchain-breaks-out/) ("[B]ecause everyone can see the block chain, anyone can spot a duplicate or fraudulent transaction.").

74. *See* J.H. WITTE, THE BLOCKCHAIN: A GENTLE INTRODUCTION 2 (2016), https://ssrn.com/abstract=2887567.

only the rightful recipient can access that value.[75] Conceptually, a public key is akin to a traditional post office box address to which anyone can send value (bitcoin or other cryptocurrencies, smart contracts,[76] titles to land, contracts for goods or services, etc.).[77] Once sent, only the private key can unlock the mailbox and retrieve that value, making the entire system secure.[78]

There is no centralized authority on the blockchain to unilaterally determine the validity of the transactions.[79] Instead, participants in the network must agree on the validity of each block (a block is simply a collection of transactions) through a decentralized consensus protocol.[80] This "trustless-trust" is really the heart of what makes the blockchain so powerful—the ability for parties, who do not know or trust one another, to conduct a transaction knowing that it will be recorded accurately, immutably, and permanently.[81] This is a big step forward from the current norm where centralized financial institutions, like banks, maintain sole control over the ledger systems

---

75. *Id.* at 1.

76. *See* NICK SZABO, SMART CONTRACTS: BUILDING BLOCKS FOR DIGITAL MARKETS (1996), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html ("The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a beginner's level problem in design with finite automata, dispense[s] change and product fairly.").

77. *Id.* ("A fundamental problem we will see throughout these protocols is the need to keep keys secret, and *pubilic key* cryptography helps solve this. In this technique, Alice generates two keys, called the private and public keys. She keeps the private key secret and well protected, and publishes the public key. When Bob wishes to send a message to Alice, he encrypts a message with her public key, sends the encrypted message, and she decrypts the message with her private key.").

78. *Id.* ("The private key provides a "trapdoor" that allows Alice to compute an easy inverse of the encryption function that used the public key. The public key provides no clue as to what the private key is, even though they are mathematically related.").

79. *See* BITCOIN WHITE PAPER, *supra* note 35, at 4.

80. *Id.* at 3–4.

81. *See* Baker, *supra* note 48, at 357.

used to track transactions and are the sole arbiters of the validity of any given transaction on the ledger.[82]

The blockchain solves a critical problem that has existed since the beginning of time: how do two parties, who do not know or trust one another, complete a transaction and ensure that they each receive what they bargained for? Traditionally this has been done by injecting a neutral intermediary into the process—the individual parties may not trust one another, but both can agree to trust a supposedly neutral third-party to broker the transaction.[83] The blockchain turns this idea on its head by removing the third-party intermediary and instead allowing the participants in the network to reach a consensus regarding the validity of each block of transactions on their own.[84] Validity, permanence, and immutability are built into the structure of the blockchain.[85] Once transactions are verified and recorded to the blockchain, it is difficult to the point of being nearly impossible for them to be changed, altered, or deleted.[86] This near immutability results from linking blocks together with cryptographic hashes and using a distributed timestamp server.[87]

So how does the blockchain facilitate this consensus and ultimately provide this "trustless-trust"? The answer lies in the second major innovation in Nakamoto's white paper—a new way of addressing the so-called "Byzantine Generals Problem." The problem describes a situation where several divisions of the Byzantine Army, each led by a different general, surround an enemy encampment.[88] The generals are physically separated from one another and can only communicate through messengers.[89] Nonetheless, the generals must

---

82. *See* Bob Blain, *The Root of U.S. Public and Private Debt, as Told by the Pen of History*, 28 MICH. SOC. REV. 70, 79 (2014) (describing a bank's practice of granting compounding interest on a savings account by using the money in the savings account as credit to bank customers, with both the balance of the creditor's account and the debtor's obligation reflecting on the bank's private ledger).

83. *See* BITCOIN WHITE PAPER, *supra* note 35, at 2.

84. *Id.*

85. *See id.* at 2–6.

86. *See id.* at 3.

87. *Id.* at 2–3.

88. AARON WRIGHT & PRIMAVERA DE FILIPPI, DECENTRALIZED BLOCKCHAIN TECHNOLOGY AND THE RISE OF LEX CRYPTOGRAPHIA 5–6 (2015) (citing Leslie Lamport et al., *The Byzantine Generals Problem*, 4 ACM TRANSACTIONS ON PROGRAMMING LANGUAGES & SYSTEMS 382, 382 (1982)), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664&rec=1&srcabs=2631314&alg=1&pos=5.

89. *Id.* at 6.

collectively decide whether to attack or to retreat.[90] If their decision is not unanimous, such that some attack and some retreat, the entire army will be defeated.[91] This problem is complicated by the fact that bad actors who wish to see the army defeated may try to interject themselves into the communications between generals.[92] Thus, the generals have to find a way to reach consensus on the battle plan, taking into account the potential for injection of bad information from actors who wish to see the army defeated.[93]

To succeed, the generals must create a system that balances the need to accept truthful communications (e.g., an honest messenger says that General 1 wants to attack), with the need to filter out false messages, (e.g., a dishonest messenger says that General 1 wants to attack when two previous messengers said that General 1 wants to retreat, in combination with messengers from General 2 and General 3 who both say that they want to retreat).[94] This balancing process is known as Byzantine Fault Tolerance,[95] and Nakamoto's white paper provides a solution to this problem using digital signatures in the distributed consensus protocol known as "proof of work."[96] The proof of work protocol provides a solution to the Byzantine Generals Problem by creating economic incentives for participants in the network to create an accurate ledger by including only valid transactions and excluding invalid transactions injected by bad actors.[97]

In a proof of work system, computers on the network that control significant processing power known as "miners" compete to validate blocks of transactions by solving complex cryptographic puzzles.[98] This is done by putting the transactions to be included in the block

---

90. *Id.* at 5–6.

91. *See id.*

92. *Id.* at 6.

93. *Id.*

94. *See id.* at 5–7.

95. *See* Justin Connell, *On Byzantine Fault Tolerance in Blockchain Systems*, CRYPTO INSIDER (June 13, 2017), https://cryptoinsider.21mil.com/byzantine-fault-tolerance-blockchain-systems/.

96. *See* BITCOIN WHITE PAPER, *supra* note 35, at 3–4. While there are other types of decentralized consensus protocols, proof of work underpins the two most popular public blockchain platforms: Bitcoin and Ethereum. *See Proof of Work vs Proof of Stake: Basic Mining Guide*, BLOCKGEEKS, https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/ (last visited Nov. 8, 2018) ("Proof of work is not only used by the bitcoin blockchain but also by ethereum and many other blockchains.").

97. *See* BITCOIN WHITE PAPER, *supra* note 35, at 3–4.

98. *See id.*

along with an arbitrary number into a hash function.[99] A hash function is nothing more than an algorithm that takes an alpha-numeric data input of any length and creates an alpha-numeric output of a specific fixed length called a hash.[100] Thus, whether the initial input is one, ten, or ten thousand characters, the output will always be the same length.[101] The resulting hash of the block is compared against the target value, a string with a certain number of zeros in front of it.[102] If the resulting hash is incorrect, the miner must guess a different arbitrary number and complete the computation again.[103]

The competition is "won" once a miner solves the hash with the correct number of zeros in front of the string.[104] While this seems simple in theory, in the case of bitcoin, it is designed to take approximately ten minutes for one block to be verified.[105] The first miner to solve the puzzle and to get a majority of the other nodes on the network to validate its solution for the arbitrary number is rewarded with a small amount of cryptocurrency—for instance, bitcoin on the Bitcoin blockchain or ether, the native currency of the

---

99. *Id.* at 3.

100. GARETH W. PETERS & EFSTATHIOS PANAYI, UNDERSTANDING MODERN BANKING LEDGERS THROUGH BLOCKCHAIN TECHNOLOGIES: FUTURE OF TRANSACTION PROCESSING AND SMART CONTRACTS ON THE INTERNET OF MONEY 4 (2015), https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2692487; *see also* J. Lawrence Carter & Mark N. Wegman, *Universal Classes of Hash Functions*, 18 J. COMPUTER & SYS. SCI. 143, 143 (1979) (discussing the creation of the different types of hash functions).

101. *See* PETERS & PANAYI, *supra* note 100, at 4. Hash functions are powerful because while identical hash inputs will always produce the same hash output, it is very difficult to derive the input from the output. To do so, you would need to make random guess after guess until you stumble on the initial input or on another input that produces the same hash. This is called a hash collision, and while technically feasible, it requires such a large amount of processing power that, with current technology, it is nearly impossible. *See* MARC PILKINGTON, BLOCKCHAIN TECHNOLOGY: PRINCIPLES AND APPLICATIONS 7 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660; WITTE, *supra* note 74, at 2.

102. *See* BITCOIN WHITE PAPER, *supra* note 35, at 3.

103. *See id.*

104. *Id.*

105. *Id.* The number of hashes computed per second is referred to as hash rate; at time of writing, the Bitcoin blockchain has a network hash rate of more than 9.8 exahash per second, which translates to 9.8 quintillion hashes per second (9.8 x 1018 solutions per second). *See Bitcoin Network Hashrate Chart and Graph*, COINWARZ, https://www.coinwarz.com/network-hashrate-charts/bitcoin-network-hashrate-chart (last visited Nov. 8, 2018).

Ethereum blockchain.[106] This "reward" creates an economic incentive for miners to be honest actors, as miners know that at least 51% of all nodes must agree that the block is valid before the miner can collect the reward.[107]

On the blockchain, the hash of each individual block is linked by reference to the hash of the previous block—thus creating a block chain.[108] This chain between the preceding and following blocks ensures the immutability of the blockchain, because a bad actor seeking to change a single transaction on the blockchain would not only have to break the encryption of that block, but would also have to change every subsequent block in the chain.[109] It would take an incredible amount of processing power to carry out this type of attack, and while certainly possible, it would require a combined effort on the part of numerous large actors on the blockchain, thus making a successful attack of this kind unlikely.[110]

To understand how this works practically, let us return to our prior example of Party A buying widgets from Party B. As we saw before, in our current credit card system, this transaction took numerous steps and involved at least three separate intermediaries to complete the transaction.[111] In contrast, on the blockchain, the

---

106. *See* BITCOIN WHITE PAPER, *supra* note 35, at 4.

107. *Id.* at 1, 4–5; *see also supra* note 66 and accompanying text.

108. BITCOIN WHITE PAPER, *supra* note 35, at 2–3.

109. *Id.* at 3.

110. As discussed above, this vulnerability, known as a 51% attack, is theoretically possible. *See supra* note 66. But it is very difficult for a single actor to amass sufficient computing power to mount such an attack. It is possible, however, using the concept of "mining pools." A mining pool is a method whereby individuals with computing power combine their power to gain a greater number of block creation rewards. These collective rewards are then divided pro-rata amongst the different contributors who assisted in validating that block. Currently, these pools hold an incredible amount of computing power, which makes 51% attacks technically feasible if the entire pool worked in concert. The 51% attack problem is a side effect of proof-of-work that plagues all major, mineable coins. *See, e.g.*, *Bitcoin Hashrate Distribution*, BLOCKCHAIN, https://blockchain.info/pools (last visited Nov. 8, 2018) (requiring four pools in collusion to mount a 51% attack); *Decred Network Hashrate Distribution*, DCR STATS, https://dcrstats.com/pow (last visited Nov. 8, 2018) (requiring two pools to mount a 51% attack); *Ethereum Top Miners*, ETHERCHAIN, https://www.etherchain.org/charts/miner (last visited Nov. 8, 2018) (requiring two pools in collusion to mount a 51% attack); *Litecoin Hash Distribution*, LITECOINPOOL, https://www.litecoinpool.org/pools (last visited Nov. 8, 2018) (requiring two pools in collusion to mount a 51% attack); *Welcome to SiaMining!*, SIAMINING, https://siamining.com (last visited Nov. 8, 2018) (requiring a single pool in collusion to mount a 51% attack).

111. *See* BITCOIN WHITE PAPER, *supra* note 35, at 1.

same transaction can be completed in two easy steps: Party A sends payment to Party B's public address on the blockchain, and Party B accesses those funds by using its private key.[112] The transaction is protected through public-private key encryption, which ensures that only the person with the private key can unlock the value.[113] The transaction is transparent, so every node on the blockchain sees and records it, making it impervious to an attack on one node or central server.[114] Moreover, the transaction is recorded in a block of transactions that are linked to the preceding and following blocks, making it difficult to retroactively change or delete any one transaction.[115]

D. The Ethereum Platform

Beginning in 2014, a small group of software developers began building a new platform for human interaction called Ethereum.[116] Whereas the Bitcoin network was specifically built as a platform for cryptocurrency exchange, Ethereum is a general purpose public blockchain on which "[a]nyone can upload programs and data and execute any program deployed to it by anybody."[117] The addition of a full programming language allows the Ethereum blockchain to run decentralized software applications ("DAPPs") that interact with one

112. *Id.*

113. *Id.* at 3–5.

114. *Id.* at 3.

115. *Id.* at 2–3.

116. *See* VITALIK BUTERIN, ETHEREUM WHITE PAPER: A NEXT-GENERATION SMART CONTRACT AND DECENTRALIZED APPLICATION PLATFORM 1 (2013) [hereinafter ETHEREUM WHITE PAPER], http://blockchainlab.com/pdf/Ethereum_white_paper a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf; HENNING DIEDRICH, ETHEREUM: BLOCKCHAINS, DIGITAL ASSETS, SMART CONTRACTS, DECENTRALIZED AUTONOMOUS ORGANIZATIONS 27–28 (2016).

117. DIEDRICH, *supra* note 116, at 27–33 ("[W]ith Ethereum you are free to really program, anything, and your scripts running on the blockchains can be applications that own money and never stop. It's [sic] purpose is to be able to do everything any other blockchain can, and then some. . . . You can program prediction markets, reputations systems, new digital currencies or a land title registry all directly on the blockchain . . . . Ethereum is a platform for decentralized applications, smart contracts and decentralized, autonomous organizations. That's a mouthful—basically it is about programs being unstoppable, incorruptible and able to make irreversible payments, which can be used to craft business agreements, a.k.a. contracts, that can be said to *execute themselves*. Without needing banks, notaries or lawyers, even in cases where things turn out very different from what was expected. Eventually, it's about the new opportunity to build self-sustaining, economic entities that 'live' on the chain and offer real-world services: the *DAOs*.").

another through the use of self-executing and self-enforcing smart contracts.[118]

With the Ethereum platform in place, entrepreneurs began searching for a way to fund the development of DAPPs to run on the network.[119] Bypassing traditional venture capital firms and initial public offerings in favor of issuing their own native crypto-tokens through ICOs, innovative developers have created opportunities for investment not in finished, easily monetized products, but in early stage ideas and concepts.[120] This ability to raise funds based on an investor's belief in an idea, instead of a venture capital fund's search for profits, has the potential to democratize not only the opportunities for early stage investment, but also the ability of innovative entrepreneurs to bring their ideas to market.

So who is building this new infrastructure? While certainly not a homogeneous group, many core blockchain developers are longtime advocates of cryptography and have been heavily influenced by both crypto-anarchist and libertarian viewpoints.[121] This has resulted in an underlying ethos of extreme skepticism, if not down-right hostility to government regulation or intervention.[122] Not surprisingly, this

---

118. *Id.*; *see also* Vitalik Buterin, *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*, ETHEREUM FOUND. (May 6, 2014), https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

119. *See* GAVIN WOOD, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER 4–6, 9 (2014) [hereinafter ETHEREUM YELLOW PAPER], https://pdfs.semanticscholar.org/ac15/ea808ef3b17ad754f91d3a00fedc8f96b929.pdf.

120 ANDREAS BOGNER, MATHIEU CHANSON & ARNE MEEUW, A DECENTRALISED SHARING APP RUNNING A SMART CONTRACT ON THE ETHEREUM BLOCKCHAIN 177 (2016), http://cocoa.ethz.ch/downloads/2017/08/2306_Sharing_App_Final_Publication.pdf.

121. *See* Baker, *supra* note 48, at 356, 371 (discussing how blockchain's "role in our social structure lives somewhere in the middle ground between crypto anarchy and the skepticism of traditional conservatism" and noting that "[p]articipation in crypto culture is a form of counter-culture and rebellious political expression, one that has developed in the vacuum created by repeated breaches of trust by the traditional institutions that surround us").

122. *Id.* at 365 ("Trustless systems challenge the need for sovereignty in cyberspace by cultivating democratized, libertarian free markets. This is the version of anarchy promised by the crypto anarchists: '[t]he leading idea is that as more and more of our transactions take place behind the veil of encryption, it becomes easier and easier for persons to undertake business relations that escape the purview of traditional nation states.'" (quoting Peter Ludlow, *New Foundations: On the Emergence of Sovereign Cyberstates and Their Governance Structures*, *in* CRYPTO ANARCHY, CYBERSTATES, AND PIRATE UTOPIAS 1, 4–5 (Peter Ludlow ed., 2001))); *see also id.* at 366 ("Freedom from the 'shadow of law' is extremely attractive to users of

ethos has given birth to blockchain platforms that through their very architecture make external regulation from traditional governmental authorities difficult.[123] Many core blockchain developers, including many involved in developing the Ethereum platform, have adopted the view that public blockchains should eschew outside government regulation and instead be governed by rules embedded within the code.[124] Relying on the idea of automated governance (commonly referred to as "code is law"), much of the new decentralized architecture has been built to thwart sovereign governments from effectively enforcing their own laws and regulations across the quickly growing ecosystem of blockchain platforms.[125]

This idea of code as law comes to life on the Ethereum platform, which allows nodes on the network to send and receive self-executing and self-enforcing smart contracts.[126] Once launched, these contracts cannot be stopped.[127] Not by the party who launched them, not by any central authority (because there isn't one), and certainly not by government regulators or law enforcement.[128] These unstoppable, self-executing smart contracts present significant regulatory and law enforcement challenges because Ethereum participants interact

---

crypto systems such as Bitcoin."); Hughes, *supra* note 44 ("Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.").

123. *See, e.g.*, Josias N. Dewey & Michael D. Emerson, *Beyond Bitcoin: How Distributed Ledger Technology Has Evolved to Overcome Impediments Under the Uniform Commercial Code*, 47 UCC L.J. 105 (2017) ("Given the decentralized nature of distributed ledgers, the U.S. government is relatively helpless to end the practice, except for those operating inside the United States or jurisdictions with U.S. friendly extradition treaties.").

124. ETHEREUM YELLOW PAPER, *supra* note 119, at 1.

125. *See* Baker, *supra* note 48, at 373 ("[T]he intense motivations of those who seek to utilize crypto systems to cultivate total libertarian economies will continue to outpace any response by law enforcement.").

126. *See* ETHEREUM WHITE PAPER, *supra* note 116, at 1, 13, 20.

127. *See* Mary Juetten, *Legal Technology and Smart Contracts: Blockchain & Smart Contracts (Part IV)*, FORBES (Sept. 6, 2017, 8:00 AM), https://www.forbes.com/sites/maryjuetten/2017/09/06/legal-technology-and-smart-contracts-blockchain-smart-contracts-part-iv/#3a6fc6826a5f.

128. *See id.* ("The principal aim of the smart contract is a tamper-proof, unambiguous, computable contractual relationship whose payout (or other outcome) automatically occurs after some pre-specified event and that once started cannot be stopped, even by injunction.").

pseudonymously.[129] Parties to a transaction are identified only by their public keys, and participants may be located anywhere in the world because the blockchain is global and respects no sovereign boundaries. In addition to the built-in pseudonymity of the blockchain, participants may further protect their anonymity by obscuring the source of any transaction through the use of a tumbler, which mixes together transactions in order to obscure their individual origins.[130] Due to this combination of pseudonymous participation and self-executing smart contracts, the Ethereum blockchain presents a significant challenge to outside interference, governmental or otherwise.[131]

That is not to say that blockchain participants are completely impervious to outside governmental intervention. The blockchain is pseudonymous, not truly anonymous, meaning that transactions between public keys on the blockchain are anonymous, but that anonymity is relinquished when a user seeks to exchange cryptocurrency for fiat currency.[132] Thus, public exchanges are the chokepoint in the system where regulators and law enforcement can insert themselves.[133] Currently, under U.S. law, exchanges that facilitate trades between cryptocurrencies and fiat currencies are considered money services businesses and are subject to know your customer and anti-money laundering requirements.[134] This transparency at the exchange level, combined with the self-identification that accompanies public marketing for a token offering,

---

129. *See* Dewey & Emerson, *supra* note 123 ("Given the pseudo-anonymous nature of Bitcoin it is incredibly difficult to trace.").

130. *See id.* ("This is especially true if it has been passed through a tumbler site, the purpose of which is to obfuscate any connection from the sender address to the recipient address after the Bitcoins have been comingled with many others.").

131. *Id.*

132. *See Bitcoin Transactions Aren't as Anonymous as Everyone Hoped*, MIT TECH. REV. (Aug. 23, 2017), https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/. Fiat currencies are what you probably think of as traditional money. They are minted and backed by central governments—examples include the U.S. Dollar and the Euro. *See* Ethan D. Jeans, *Funny Money or the Fall of Fiat: Bitcoin and Forward-Facing Virtual Currency Regulation*, 13 COLO. TECH. L.J. 99, 103 (2015) ("[F]iat currencies rely on the authority of a sovereign government's word.").

133. *See* Jeans, *supra* note 132, at 103.

134. U.S. DEP'T OF THE TREASURY, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf; *see also BSA Requirements for MSBs*, U.S. DEP'T OF THE TREASURY, https://www.fincen.gov/bsa-requirements-msbs (last visited Nov. 8, 2018).

ensures that law enforcement have little trouble identifying and prosecuting outright fraud perpetrated by those who launch fraudulent ICOs as a quick way to scam unsuspecting investors.[135] Nevertheless, by keeping the proceeds of their fraud in cryptocurrencies or exchanging their cryptocurrency to fiat currency through a private transaction, more sophisticated operators could likely escape outside governmental regulation or prosecution through the exploitation of the pseudonymity that is a core component of public blockchains.[136]

These built-in defenses to outside regulation are important in discussing the emergence of ICOs and early attempts by government regulators to assert their authority into this space. While regulators can interject themselves at the exchange chokepoints, whether the SEC or other regulators would have much success in actually enforcing securities laws against blockchain participants who actively seek to avoid enforcement remains unclear.[137] Remember, The DAO was formed without incorporating or having a centralized management structure or identified directors. And the names and identities of its members were protected through the pseudonymity provided by the blockchain.[138] But for the public and transparent efforts of those who promoted The DAO, it is possible that regulators would have struggled to identify any single person or entity that was responsible for its formation.[139] In such a situation, it is unclear who would be the target of such an enforcement action.[140]

---

135. *See* FED. BUREAU OF INVESTIGATION, BITCOIN VIRTUAL CURRENCY: UNIQUE FEATURES PRESENT DISTINCT CHALLENGES FOR DETERRING ILLICIT ACTIVITY (2012), https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf; *see also* EDWARD V. MURPHY, M. MAUREEN MURPHY & MICHAEL V. SEITZINGER, BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 21 (2015), https://fas.org/sgp/crs/misc/R43339.pdf.

136. *See* Baker, *supra* note 48, at 373.

137. *Id.*

138. *See* SEC REPORT, *supra* note 18, at 6.

139. It is also possible, if not likely, that without such efforts The DAO would not have raised such a significant amount of funds. That said, the larger point still remains—we now live in a world where entities can be formed and operate pseudonymously.

140. *See* Hinkes, *supra* note 4.

II. INITIAL COIN OFFERINGS

Initial coin offerings have exploded as the preferred mechanism used by blockchain entities to raise funds.[141] ICOs represent a new form of crowdfunding whereby participants exchange existing cryptocurrencies (usually bitcoin or ether) for entity-specific crypto-tokens.[142] Initial coin offerings are most often compared to initial public offerings ("IPOs"), the process though which companies sell stock shares to the public for the first time.[143] Both are used to raise funds for budding companies, both can produce eye-popping hauls of cash, and both have the potential to make company founders instantly wealthy.[144] That, however, is where the similarities end. IPOs are subject to registration and ongoing compliance requirements under the Securities Act of 1933 and the Securities Exchange Act of 1934 (collectively, the "Acts").[145] The Acts aim to ensure securities sellers provide truthful and accurate information so that the public can make informed investment decisions.[146] Because of the Acts' extensive and at times complex requirements, launching an IPO in the United States is a months-long process that requires hiring an investment bank and legal counsel.[147] The Acts require that all securities offered to the public either be registered with the SEC or meet one of several enumerated exemptions to registration.[148]

In the traditional world of capital raises, companies with exciting ideas for new products or services first have to build a prototype or

---

141. *See* Russo, *supra* note 17. Initial coin offerings are sometimes referred to as "token offerings" or "token sales." Additionally, there are numerous names for the digital assets issued through ICOs, including cryptographic coins, cryptographic tokens, and blockchain tokens. For clarity and consistency, this Article will refer to these assets as either crypto-tokens or tokens.

142. *See Investor Bulletin: Initial Coin Offerings*, *supra* note 18.

143. *See* Erin Griffith, *Why Startups Are Trading IPOs for ICOs*, FORTUNE (May 5, 2017), http://fortune.com/2017/05/05/ico-initial-coin-offering/.

144. *Id.*

145. *See* 15 U.S.C. § 77(b)–(c) (2012).

146. *See* Jeffrey E. Alberts & Bertrand Fry, *Is Bitcoin a Security?*, 21 B.U. J. SCI. & TECH. L. 1, 4–5 (2015) ("[A]n essential purpose of the Securities Act is to create a framework of regulations with the aim of ensuring that issuers and sellers of securities provide investors with adequate and accurate information upon which to base their investment decisions.").

147. *See id.* ("Registration of securities under the Securities Act is time-consuming, expensive, and typically necessitates the involvement of attorneys, accountants, and other professionals.").

148. *See* 15 U.S.C. § 77(e) (2012).

beta to demonstrate to investors the validity of their idea.[149] Only after having a functioning product or service and usually only after having some level of adoption of that product or service can a company seek out venture funding to further develop or scale the idea.[150] Entrepreneurs are then forced to give up significant equity in their own creations in exchange for early seed round capital.[151] All of this occurs before entrepreneurs can even think about an initial public offering. This structure limits who can develop new ideas because entrepreneurs without connections to early stage investors are unlikely to raise the capital needed to be successful.[152] It also limits who can provide investment to early stage companies because most early round raises are limited by U.S. securities laws to wealthy accredited investors.[153] Thus, the rich and well connected get richer, and less fortunate entrepreneurs see good ideas die before ever having the chance to become a reality.

ICOs represent a fundamental shift in the way ideas are developed and commercialized by allowing developers with strong ideas for new decentralized applications, products, or services on the blockchain to raise funds from those who would ultimately utilize the application, product, or service being built.[154] This differs significantly from traditional IPOs and other early stage capital funding

149. *See* Thomas Murphy, *Playing to a New Crowd: How Congress Could Break the Startup Status Quo by Raising the Cap on the Jobs Act's Crowdfunding Exemption*, 58 B.C. L. REV. 775, 784 (2017) ("[V]enture capitalists generally do not make their funds available for the initial growth needs of a startup, which means that an entrepreneur will likely have to turn to other sources of capital to operate at least until he or she is established enough to be considered by a venture capitalist.").

150. *See id.*

151. *See id.* at 783 ("The sophisticated investors who operate venture capital funds take large ownership stakes in early-stage startups . . . .").

152. *Id.* at 779 ("[T]he lack of gender and racial diversity in the entrepreneurial landscape in the United States makes survival more difficult for entrepreneurs who do not fit the startup financing status quo of primarily white men from elite universities. Traditional sources of capital for entrepreneurs have historically been effectively unavailable to women and minorities."); *see also id.* at 784 ("In most cases, an entrepreneur will need to network his or her way into an introduction with a venture capitalist before their startup will be seriously considered for venture financing.").

153. *See* Max E. Isaacson, *The So-Called Democratization of Capital Markets: Why Title III of the JOBS Act Fails to Fulfill the Promise of Crowdfunding*, 20 N.C. BANKING INST. J. 439, 441 (2016) (discussing how, even following the passage of the Jobs Act, "offerings to non-accredited investors have been relatively nonexistent").

154. *See* Stan Schroeder, *The ICO Is a Revolutionary New Way to Get Funded, and Everyone Wants In*, MASHABLE (June 18, 2017), http://mashable.com/2017/06/18/ico-explained/#0ssxy_0c35q8.

mechanisms. First, in most ICOs, the issued tokens do not grant purchasers any form of equity or ownership interests in the issuing company.[155] Instead, most ICOs issue some form of what the industry has termed a "utility token."[156] Utility tokens are entity-specific crypto-assets that have some utility within the software application or platform being developed.[157] Utility tokens can be used to power decentralized applications built on the Ethereum blockchain or to purchase products or services on the issuing entity's decentralized software or protocol.[158] Although often times designed to be used as payment within the issuing entity's blockchain ecosystem, utility tokens may also operate as an independent store of value that can be traded through online cryptocurrency exchanges.[159] In this way, ICOs are less akin to IPOs and more closely related to pre-orders or even gift card sales, with purchasers ostensibly buying tokens that will have value within the issuing entity's system once the system is actually built.

ICOs also differ from IPOs in that, to date, they largely have not complied with any of the registration or disclosure requirements under U.S. securities laws.[160] Nonetheless, recent ICOs have raised immense sums of money.[161] Numerous ICOs have been launched by companies with no established track record, no history of bringing a

---

155. *See id.* ("But tokens don't typically give their owners ownership over a part of the company that issued them.").

156. *See* Laura Shin, *Are ICOs for Utility Tokens Selling Securities? Prominent Crypto Players Say Yes*, FORBES (Oct. 2, 2017, 9:15 AM), https://www.forbes.com/sites/laurashin/2017/10/02/are-icos-for-utility-tokens-selling-securities-prominent-crypto-players-say-yes/#56625bf234fa.

157. *Id.*

158. *Id.*

159. *See, e.g.*, *A Securities Law Framework for Blockchain Tokens*, COINBASE (Dec. 7, 2016), https://www.coinbase.com/legal/securities-law-framework.pdf.

160. *See* Securities Act of 1933, 15 U.S.C. §§ 77a–77bbbb (2012); Securities Exchange Act of 1934, 15 U.S.C. §§ 78a–78pp (2012); *see also* Jay Clayton, *Statement on Cryptocurrencies and Initial Coin Offerings*, U.S. SEC. & EXCH. COMM'N (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11 ("Investors should understand that to date no initial coin offerings have been registered with the SEC. The SEC also has not to date approved for listing and trading any exchange-traded products (such as ETFs) holding cryptocurrencies or other assets related to cryptocurrencies. *If any person today tells you otherwise, be especially wary.*").

161. *See, e.g.*, Shin, *supra* note 13, at 64; *see also* Vitalik Buterin (@VitalikButerin), TWITTER (June 12, 2017, 8:23 PM), https://twitter.com/vitalikbuterin/status/874467356734504962?lang=en ("There's no 'cure' for bubbles except to let them run their course and pop, unfortunately.").

viable product to the marketplace, and little more than an idea expressed in a white paper or a few lines of code.[162] There have even been ICOs—like The DAO's token sale—launched by developers without ever forming a corporation or other legal entity.[163] Other ICOs have completed multi-million dollar raises by marketing tokens that are explicitly held out as having no "rights, uses, purpose, attributes, functionalities or features."[164]

ICOs have become a target for governments around the world.[165] This is in part because in some (but not all) offerings, investors are allowed to purchase crypto-tokens pseudonymously.[166] This pseudonymity presents challenges to governmental regulators

---

162. *See, e.g.*, Shin, *supra* note 13, at 66 (comparing the ICO boom to the first internet bubble where "companies with more concept than concrete [business plans], day-trader speculators, wild volatility, Dutch auctions, instant fortunes created out of thin air—were ubiquitous").

163. *See id.* at 67 ("The entities raising money in these coin offerings are not always startups. Sometimes they're merely developers collaborating on a project and don't form a legal entity.").

164. *See* EOS, EOS TOKEN PURCHASE AGREEMENT 3 (Sept. 4, 2017), https://eos.io/documents/block.one%20-%20EOS%20Token%20Purchase%20Agreement%20-%20September%204,%202017.pdf. It is unclear exactly what an EOS token is. *Id.* We know, however, what it is not from the purchase agreement, which states that tokens "have no rights, uses, purpose, attributes, functionalities or features," *id.* at 8, that the tokens "may have no value," *id.*, that "[a]lthough EOS Tokens may be tradable, they are not an investment, currency, security, commodity, a swap on currency, security or commodity or any other kind of financial instrument," *id.* at 3, that "[b]uyer[s] should not participate in the EOS Token Distribution or purchase EOS Tokens for investment purposes," *id.* at 4, and buyers must "acknowledge[] and agree[] that Buyer is not purchasing EOS Tokens for purposes of investment, speculation, as some type of arbitrage strategy, for immediate resale or other financial purposes," *id.* at 5. Despite the tokens being sold as having no value and no utility, the ICO still raised in excess of $185 million in less than five days. *See* Marshall, *supra* note 11.

165. Many countries are skeptical towards cryptocurrencies and ICOs. *See* Chrisjan Pauw, *In Wake of China ICO Ban, Japan, Singapore, US Give Crypto Second Look*, COINTELEGRAPH (Sept. 15, 2017), https://cointelegraph.com/news/in-wake-of-china-ico-ban-japan-singapore-us-give-crypto-second-look. Some countries have seen fit to ban all ICOs. *See* Brenda Goh & Elias Glenn, *Cryptocurrency Chaos as China Cracks down on ICOs*, REUTERS (Sept. 12, 2017), https://www.reuters.com/article/us-china-finance-digital-ico-analysis/cryptocurrency-chaos-as-china-cracks-down-on-icos-idUSKCN1BN33R; *see also* Russell, *supra* note 23. Other countries have gone a step further, banning all cryptocurrency exchanges except for those officially sanctioned by the state. *See* Stan Higgins, *Russia's Central Bank Issues Warning on Cryptocurrencies and ICOs*, COINDESK (Sept. 5, 2017, 16:35 UTC), https://www.coindesk.com/russias-central-bank-issues-warning-cryptocurrencies-icos/.

166. *See* SEC REPORT, *supra* note 18, at 6.

seeking to enforce tax and banking laws and raises the potential for illegal uses, including criminal money laundering and covert terrorism funding.[167] While this potential for illegality is real, studies have found that illicit activity represents only a fraction of the transaction volume on public blockchains (as it does in the real world) and thus, should not serve as justification for squashing the real innovation occurring in this space.[168] The mainstream media—which has at times demonstrated a lack of understanding of how public blockchains operate—often sensationalizes illegality on the blockchain, thereby creating confusion amongst the general public.[169] In reality, while fraudsters, money launderers, drug dealers, and other miscreants certainly utilize public blockchain platforms, this accounts for only a small fraction of blockchain activity.[170] Thus, while we must be mindful of how this technology can facilitate illegal acts, we should be careful not to overstate this threat.

---

167. *See* Baker, *supra* note 48, at 371 ("Crypto anarchy promises liberation from state and institutional oversight, but it also carries with it very real dangers, and provides a means for a plethora of illegal activity such as tax evasion, money laundering, theft of trade secrets, and serious national security and terrorism risks.").

168. *See* YAYA J. FANUSIE & TOM ROBINSON, BITCOIN LAUNDERING: AN ANALYSIS OF ILLICIT FLOWS INTO DIGITAL CURRENCY SERVICES 2 (2018), http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf ("The amount of observed Bitcoin laundering was small (less than one percent of all transactions entering conversion services) . . . ."); *see also* Nicolas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* 17–20 (Carnegie Mellon INI/CyLab, Working Paper No. 1654, 2012), https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf (concluding that the Silk Road's monthly revenue totaled only $1.2 million and represented only 4.5% of all bitcoin transactions occurring in exchanges).

169. *See, e.g.*, Bart Chilton, *It's Time to Address Bitcoin's Big Blind Spot*, CNBC (Sept. 21, 2017, 3:10 PM), https://www.cnbc.com/2017/09/21/its-time-to-address-bitcoins-big-blind-spot-bart-chilton-commentary.html (former U.S. Trading Commissioner using the Silk Road crackdown and Mt. Gox failure to argue for increased regulation of cryptocurrencies); Arjun Kharpal, *Robot with $100 Bitcoin Buys Drugs, Gets Arrested*, CNBC (Apr. 21, 2015, 6:59 AM), https://www.cnbc.com/2015/04/21/robot-with-100-bitcoin-buys-drugs-gets-arrested.html; Maria Perez, *NYC Federal Officials Confiscate $48 Million from Silk Road Creator*, NEWSWEEK (Sept. 30, 2017, 3:32 PM), http://www.newsweek.com/nyc-federal-officials-confiscate-48-million-silk-road-creator-675012.

170. *See* FANUSIE & ROBINSON, *supra* note 168, at 2.

III. THE SEC'S REPORT ON THE DAO

On July 25, 2017, the SEC released its eighteen-page report on The DAO.[171] Utilizing the 1946 Supreme Court decision in *Howey*,[172] the SEC concluded that DAO tokens were securities.[173] The DAO likely roused the SEC's attention due to its much-publicized $150 million raise coupled with the even more highly publicized cyber-exploit that drained nearly two-thirds of that value.[174] Ultimately, the Ethereum community would come to the rescue, implementing a fork in the code[175] that allowed all DAO token holders to recover their stolen funds.[176] While it is not surprising that such a high profile rise and fall would garner regulator attention, The DAO differed significantly from the majority of contemporary ICOs and as such, was not the best model for the SEC to provide an analysis that would be broadly applicable to the larger ICO marketplace. More problematic is the fact that the SEC's report ignores critical aspects of The DAO's operation and in so doing, draws conclusions that are at odds with existing case law.[177]

---

171. *See* SEC REPORT, *supra* note 18, at 1.

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

173. SEC REPORT, *supra* note 18, at 11.

174. *See, e.g.*, Ronald David Smith & David E. Barrett, *The DAO's Wild Ride: Where Does Blockchain Go from Here*, FORBES (July 1, 2016, 1:28 PM), https://www.forbes.com/sites/realspin/2016/07/01/the-daos-wild-ride-where-does-blockchain-go-from-here/#7e6864ec3e5c.

175. See *supra* note 66 and accompanying text for a general description of forking in code.

176. This involved a two-step process with a soft fork and a hard fork. The initial soft fork was aimed at preventing the exploiter from removing the ether from his sectioned-off account. It was indicated just before this fork went live that it would create security vulnerabilities in the code, which resulted in cancelling the initial soft fork. As a result, the soft fork was not implemented, and the only remaining option was to hard fork. The hard fork essentially moved the funds in The DAO to a different account that allowed DAO token holders to trade their tokens back into ether. As a result, all funds were recovered, and no DAO token holder lost their investment because of the exploit. *See* Adam Hayes, *Ethereum Reaches Consensus to Hard Fork, Fixing DAO Hack*, INVESTOPEDIA (July 19, 2016, 9:13 AM), http://www.investopedia.com/articles/investing/071916/ethereum-reaches-consensus-hard-fork-fixing-dao-hack.asp; Madeira, *supra* note 66; Joon Ian Wong & Ian Kar, *Everything You Need to Know About the Ethereum "Hard Fork,"* QUARTZ (July 18, 2016), https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/.

177. *See supra* notes 23–33 and accompanying text.

A. The DAO

The DAO was formed as the world's first truly decentralized autonomous organization—an entity (for lack of a better descriptor) that runs without a centralized management team and whose decision making is 100% entrusted to its token holders.[178] The DAO itself did not exist in any physical location and was not owned by anyone.[179] Instead it was nothing more than a smart contract, a piece of computer code, deployed on the Ethereum blockchain.[180] As articulated in the original DAO white paper, this smart contract "store[d] ether and other Ethereum based tokens and transmit[ted] them based on the DAO's code. It [did] not do much else. It [could not] build a product, write code or develop hardware."[181] Set up to provide capital investment for the development of decentralized software applications or "DAPPs" built on the Ethereum blockchain, The DAO was essentially a decentralized venture capital fund.[182]

The DAO smart contract was developed by Christoph Jentzsch, founder and chief technology officer of Slock.it, a blockchain company.[183] Jentzsch articulated his vision for a company that could run without centralized management in a white paper and later released an open-source DAO smart contract that could be used by anyone who wished to deploy it on the Ethereum platform.[184] A number of individuals and entities deployed the DAO smart contract, but the smart contract that attracted the most ether contributions (and ultimately came to be known as The DAO) was launched and promoted by Jentzsch and Slock.it.[185] Although they promoted The

---

178. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2.

179. *Id.*

180. *See* Andrew Quentson, *Are The DAO Curators Masters or Janitors?*, COIN TELEGRAPH (June 12, 2016), https://cointelegraph.com/news/are-the-dao-curators-masters-or-janitors ("In its foundations the DAO . . . is literally code.").

181. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2.

182. *Id.*

183. Slock.it is developing a "universal sharing network" that seeks to remake the sharing economy by removing the intermediaries (Airbnb, Uber, etc.) in favor of peer-to-peer transactions on Ethereum blockchain. *See* SLOCK.IT, https://slock.it/ (last visited Nov. 8, 2018).

184. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 1.

185. *See Slockit/DAO*, GITHUB, https://github.com/slockit/DAO (last visited Nov. 8, 2018) (GitHub repository created by Stephan Tual, COO and Founder of Slock.it, containing the Standard DAO Framework, which was eventually implemented in the creation of The DAO); Stephen Tual, *Vitalik Buterin, Gavin Wood, Alex van De Sande, Vlad Zamfir Announced Amongst Exceptional DAO Curators*, MEDIUM: SLOCK.IT

DAO, neither Jentzsch nor Slock.it controlled The DAO's funds or operational decisions.[186] Instead, all decisions regarding the use of DAO funds were directly controlled by DAO token holders.[187]

There were no limitations on who could purchase DAO tokens, and all contributions to The DAO were made pseudonymously, with only the contributor's public Ethereum blockchain address being visible.[188] There were also no limitations on how many DAO tokens could be purchased and no mechanism to limit the offering to knowledgeable or sophisticated investors.[189] Such an open and democratic offering stands in stark contrast to current early seed round investing that is limited to accredited investors and in reality, dominated by a small number of well-connected angel investors and venture capital funds.[190] While not immediately liquid, once the offering period ended, DAO tokens could be freely transferred on the Ethereum blockchain.[191] Slock.it "solicited at least one U.S. web-based platform to trade DAO Tokens on its system," and "promotional materials disseminated by Slock.it included representations that DAO Tokens would be available for secondary market trading after the offering period via several platforms."[192]

The DAO was not designed to produce or sell anything; instead, it would use its resources to fund other projects on the Ethereum blockchain.[193] In order to be considered for funding, a "contractor" had to first submit a specific smart contract, known as a "proposal," to The DAO.[194] Proposals would outline the development idea and request

---

BLOG (Apr. 25, 2016), https://blog.slock.it/vitalik-buterin-gavin-wood-alex-van-de-sande-vlad-zamfir-announced-amongst-stellar-dao-curators-44be4d12dd6e.

186. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2.

187. *Id.*

188. *See* SEC REPORT, *supra* note 18, at 6.

189. *Id.*

190. *See* Murphy, *supra* note 149, at 779–80 ("Although there are financing alternatives to venture capital and angel investors—the two methods traditionally used by entrepreneurs to launch new businesses—one study shows that, on average, successful startups raise $41 million from those two sources. This places entrepreneurs ignored by venture capitalists and angel investors at a significant comparative disadvantage.").

191. *See* SEC REPORT, *supra* note 18, at 6.

192. *Id.*

193. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2.

194. *Id.*; *see also* SEC REPORT, *supra* note 18, at 7 ("An individual or entity must: (1) own at least one DAO Token; and (2) pay a deposit in the form of ETH that would be forfeited to the DAO Entity if the proposal was put up for a vote and failed to achieve a quorum of DAO Token holders.").

the funds necessary to make it happen.[195] Contractors were required to post details about their proposal on The DAO Website, including the Ethereum blockchain address of the smart contract and a link to its source code.[196] This transparency allowed all DAO token holders the ability to review all submitted proposals and make informed decisions as to whether to fund specific projects.[197] Prior to DAO token holders voting to fund a project, the proposal had to first be approved by The DAO's "curators."[198] The initial group of curators was comprised of eleven individuals, all of whom were current or former members of the Ethereum project and had extensive development experience on the Ethereum platform.[199] This list included, among other notable names, Vitalik Buterin, one of the founders and chief architect of the Ethereum blockchain platform.[200] Importantly, none of the curators came from Slock.it, and DAO token holders, through a majority vote, had the power to remove any curator for any reason, as well as the power to nominate new curators.[201]

Once a proposal was "whitelisted" by a curator, DAO token holders could vote on whether to fund the proposal.[202] Each individual token holder was allowed to vote on every proposal or to abstain based on their own personal preferences.[203] Only proposals that were approved by a majority of voting token holders would be funded by The DAO.[204] Importantly, regardless of whether an individual token holder voted for, voted against, or abstained from voting on a given proposal, the token holder retained the right and ability to opt-out of approved proposals for any reason.[205] When this right was exercised, the token holder's initial ether contribution would be returned in full to the token holder.[206]

Understanding this history and The DAO's structure is critical to the *Howey* analysis because despite the SEC's emphasis on Slock.it's actions as the "promoter," this was not a typical capital raise where an individual or small group of individuals raises funds from others

---

195. *See* SEC REPORT, *supra* note 18, at 6–7.
196. *Id.* at 7.
197. *Id.*
198. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2–3.
199. *See* Tual, *supra* note 185.
200. *Id.*
201. *See id.*
202. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2.
203. *Id.*
204. *Id.*
205. *See id.*
206. *See id.*

who are relying on the actions or expertise of those promoters to produce a profit.[207] While Slock.it actively promoted The DAO, participants in its token offering did not contribute ether to Slock.it but to The DAO smart contract—a piece of computer code that was neither owned nor controlled by Slock.it, Jentzsch, or any other person or entity.[208]

DAO token holders were not investors in a company whose managers would make decisions as to how to best utilize the invested funds but instead were parties to a mutually symmetric contract that bound all participants under the same immutable terms.[209] It was the terms of this contract (and the input of consensus from token holders required by the contract) that dictated how The DAO would utilize the funds contributed by token holders and ultimately determined whether the entity would be profitable.[210] Neither Slock.it, Jentzsch, the curators, nor anyone else mentioned in the SEC's report could take any action to put individual token holder's contributed funds at risk without the approval of a majority vote of token holders.[211] And as discussed in detail below, even when such an action was approved by a majority vote, each individual token holder still retained the ability to retrieve his, her, or its contributed funds.[212]

It might be helpful to pause here in order to allow you to get your head around this: exchanging a cryptocurrency that has no physical form and is not backed by a sovereign government into a separate crypto-token with similar attributes via a smart contract that is nothing more than computer code, which sits on a network that does not physically exist anywhere, has no person or entity in charge, and acts only through the consensus of a majority of the pseudonymous individuals or entities that hold its tokens. I told you earlier that that the blockchain will challenge your conceptions about what is and is not possible; this is what I meant. What I just described is not some far-fetched sci-fi future; it has already occurred. And while the first experiment ended in failure, do not think for one second that either the technology or the individuals pushing the boundaries of this new world are going away any time soon. Now, having emerged from our trip down the blockchain rabbit hole with this understanding, let us

---

207. *See id.*
208. *See id.*
209. *See id.*
210. *See id.*
211. *See id.*
212. *See id.*

return to the more familiar confines of case law and dissect the SEC's *Howey* analysis.

B. Howey

In its 1946 decision in *Howey*, the Supreme Court articulated a three-part test for determining whether a particular transaction or arrangement was an "investment contract" and therefore a security subject to regulation under the 1933 Securities Act.[213] "[A]n investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person [1] invests his money [2] in a common enterprise and [3] is led to expect profits solely from the efforts of the promoter or a third party . . . ."[214] This definition "embodies a flexible rather than a static principle, one that is capable of adaption to meet the countless and variable schemes devised by those who seek to use the money of others on the promise of profits."[215] While the *Howey* Court used this test to conclude that a contract for the sale of orange groves paired with a service contract for cultivating and marketing the oranges constituted a security, over the intervening decades the test has been applied to a diverse and broad array of arrangements and transactions.[216]

C. Investment of Money

The SEC had little trouble concluding that DAO token holders invested money.[217] Courts have long held that the investment of money need not take the form of cash to satisfy *Howey*.[218] The SEC concluded that "[i]nvestors in The DAO used [ether] to make their investments, and DAO Tokens were received in exchange for [ether]."[219] This, the SEC concluded, "is the type of contribution of value that can create an investment contract under *Howey*."[220] I quibble not with this conclusion.

---

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

214. *Id.*

215. *Id.* at 299.

216. *See* SEC v. Glenn W. Turner Enters., 474 F.2d 476, 481 n.6 (9th Cir. 1973) (collecting cases "in which diverse schemes have been held to involve securities").

217. *See* SEC REPORT, *supra* note 18, at 11.

218. *See, e.g.*, Uselton v. Commercial Lovelace Motor Freight, Inc., 940 F.2d 564, 574 (10th Cir. 1991) ("[I]t is well-established that cash is not the only form of contribution or investment that will create an investment contract.").

219. *See* SEC REPORT, *supra* note 18, at 11.

220. *See id.*

D. Common Enterprise

While devoting several sentences and even citing case law in support of its uncontroversial conclusion that DAO token holders invested money, the SEC, without any citation to authority or analysis, reached a far more controversial conclusion in its report: DAO token holders were investing in a common enterprise.[221] In fact, the SEC did not cite to a single case in reaching its common enterprise conclusion,[222] despite the existence of a robust collection of case law addressing this element, including three different tests for commonality that are more or less embraced across varying federal jurisdictions.[223] Nor did the SEC provide any factual background or analysis describing how The DAO constitutes a common enterprise.[224] Instead, it mentioned in passing that the ether contributed by DAO token holders was "pooled and available to the DAO to fund projects."[225] At first blush, this "pooling" of token holder funds could be seen as creating a common enterprise; however, a closer examination of the structure and operation of The DAO raises serious questions as to whether an investment in DAO tokens satisfied any of the three commonality tests utilized by federal courts.

In the seventy-plus years since *Howey*, the Supreme Court has provided little guidance as to the definition of common enterprise.[226] This has left the federal circuit courts free to develop their own jurisprudence in this area, resulting in the advancement of three separate common enterprise tests: (1) horizontal commonality, (2) broad vertical commonality, and (3) strict vertical commonality.[227] While some circuits have expressly adopted a single test, others variably apply two or even all three tests.[228] Due to this lack of a single

---

221. *See id.*

222. A simple Westlaw search of cases that both contain the term "common enterprise" and cite to *Howey* turns up over 950 results.

223. *See generally* SEC REPORT, *supra* note 18.

224. *See generally id.*

225. *Id.* at 12.

226. Christopher L. Borsani, *A "Common" Problem: Examining the Need for Common Ground in the "Common Enterprise" Element of the* Howey *Test*, 10 DUQ. BUS. L.J. 1, 7 (2008).

227. *Id.*

228. *See* Travis Stegemoller, *Refocusing Commonality: An Economic Approach that Shares Something in Common with* Howey, 46 VAL. U. L. REV. 657, 676–77 (2012) ("To date, the horizontal commonality test has been adopted and regularly used by the Third, Sixth, and Seventh Circuits. Broad vertical commonality is mostly confined to the Fifth Circuit. The Eighth Circuit favors vertical commonality . . . . [T]he Ninth Circuit . . . applie[s] the strict vertical commonality test more often than the broad

agreed-upon standard, an analysis of all three formulations is necessary in order to address the question that the SEC's report simply glossed over: was The DAO a common enterprise?

Horizontal commonality is said to be the "clearest example of common enterprise," as it is based on the relationship between the investors in a transaction.[229] Horizontal commonality requires the "pooling of assets from multiple investors [so] that all share in the profits and risks of the enterprise."[230] Thus, the success of each individual investor must be tied to the success of the other individual investors in the enterprise.[231] In addition to the pooling of assets, the pooling of profits that are then distributed to individual investors pro rata "is essential to horizontal commonality."[232]

Even a cursory review of The DAO's structure makes clear that The DAO did not satisfy the horizontal commonality test. While the SEC is correct that DAO token holders' ether contributions were "pooled and available to The DAO to fund projects," [233] all individual token holders had the right to withhold their individual ether contribution from funding any particular proposal.[234] In fact, Jentzsch's white paper[235] specifically provided a mechanism for token holders to opt out of proposals and to take their entire ether contribution out of the pooled resources that would be used to fund any given proposal:

---

vertical commonality test. Interestingly, the Tenth Circuit Court of Appeals has used a combination of both vertical commonality tests while expressly rejecting horizontal commonality. In the Eleventh Circuit, it appears broad vertical commonality is favored. As for the remaining circuits—the First, Second, and Fourth Circuits—the issue has yet to be decided as all have declined the opportunity to clarify the matter even though the district courts within their circuits are inconsistent in applying one test over the others.").

229. Borsani, *supra* note 226, at 8; *see also* THOMAS LEE HAZEN, THE LAW OF SECURITIES REGULATION § 1.6[2][B] (5th ed. 2006).

230. SEC v. SG Ltd., 265 F.3d 42, 50 (1st Cir. 2001).

231. *See* Borsani, *supra* note 226, at 8–9.

232. Wals v. Fox Hills Dev. Corp., 24 F.3d 1016, 1019 (7th Cir. 1994).

233. SEC REPORT, *supra* note 18, at, 12.

234. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2.

235. The SEC grounded its factual description of The DAO and its operations in statements made in Jentzsch's white paper. *See generally* SEC REPORT, *supra* note 18. Nowhere in the SEC's report is there any indication that The DAO was structured or operated in any way inconsistent with its description in the white paper. *See generally id.* Because the SEC's factual analysis was grounded in the white paper's explanation of The DAO's operation, this Article assumes that the actual operation of The DAO was consistent with that provided in the white paper.

> If an individual, or a group of token holders, disagree with a proposal and want to retrieve their portion of the ether before the proposal gets executed, they can submit and approve a special type of proposal to form a new DAO. The token holders that voted for this proposal can then split the DAO moving their portion of the ether to this new DAO, leaving the rest alone only able to spend their own ether.[236]

This ability of individual token holders to choose on a case-by-case basis whether to participate in a given proposal demonstrates that token holders did not "share in the profits and risks of the enterprise."[237]

All actions to spend The DAO's "pooled" ether required a vote of DAO token holders.[238] Upon approval of a given proposal by 51% of voting token holders, individual token holders were allowed to opt out of the proposal and in so doing retrieve the entirety of their initial contribution.[239] If an individual or group of token holders exercised this power, they would no longer share the potential for risks or profits with other token holders who choose not to retrieve their funds.[240] This procedure was put in place to ensure that minority token holders could protect their own individual interests notwithstanding whatever action was collectively approved by a majority of token holders.[241]

In contrast to horizontal commonality, the strict vertical commonality approach shifts the focus away from the investors' shared fortunes and instead focuses on the relationship between the economic interests of the promoter and those of the individual

---

236. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2.

237. SEC v. SG Ltd., 265 F.3d 42, 50 (1st Cir. 2001). This analysis is limited to whether the sale of DAO tokens constituted a sale of securities. While there are likely strong arguments that had The DAO funded proposals (which it did not due to the cyber-attack that drained its funds), those proposals could have constituted securities sales, such an analysis is beyond the scope of this Article.

238. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2.

239. *Id.*

240. *Id.*

241. *Id.* ("A problem every DAO has to mitigate is the ability for the majority to rob the minority . . . . To prevent this, the minority must always have the ability to retrieve their portion of the funds.").

investors.[242] The concept of strict vertical commonality[243] was first articulated by the Ninth Circuit in a footnote in its seminal 1974 decision *SEC v. Glenn W. Turner Enterprises*, where it defined a common enterprise as "one in which the fortunes of the investor are interwoven with and dependent upon the efforts and success of those seeking the investment or of third parties."[244] The "hallmark of strict, or narrow, vertical commonality is the economic relationship between the investor and the promoter."[245] Thus, it need not be shown that individual investor contributions were pooled or that individual investors shared the same potential risks or profits.[246]

Whereas strict vertical commonality looks to whether investors' fortunes were intertwined with those of the promoter, broad vertical commonality looks to investors' dependence on the promoter's expertise.[247] The broad vertical commonality inquiry was first articulated in 1974 by the Fifth Circuit in *SEC v. Koscot Interplanetary, Inc.*[248] There, the court held that "the fact that an investor's return is independent of that of other investors in the scheme is not decisive. Rather, the requisite commonality is evidenced by the fact that the fortunes of all investors are inextricably tied to the efficacy of [the promoter's actions]."[249] Importantly, the *Koscot* court limited its holding "to those schemes in which promoters retain immediate control over the essential managerial conduct of an enterprise and where the investor's realization of profits is inextricably tied to the success of the promotional scheme."[250] The Fifth Circuit built on this basic principle later the same year in *SEC v. Continental Commodities Corp.*, where it held that "the critical inquiry is confined to whether the fortuity of the investments collectively is essentially dependent upon promoter expertise."[251] Fifteen years later the Fifth Circuit clarified that "the necessary

---

242. *See* Maura K. Monaghan, *An Uncommon State of Confusion: The Common Enterprise Element of Investment Contract Analysis*, 63 FORDHAM L. REV. 2135, 2157–58 (1995).

243. Strict vertical commonality may also be referred to as narrow vertical commonality. *See id.* at 2157 n.158.

244. SEC v. Glenn W. Turner Enters., 474 F.2d 476, 482 n.7 (9th Cir. 1973).

245. *See* Monaghan, *supra* note 242, at 2157.

246. *Id.*

247. James D. Gordon III, *Defining a Common Enterprise in Investment Contracts*, 72 OHIO ST. L.J. 59, 75–76 (2011).

248. 497 F.2d 473, 478 (5th Cir. 1974).

249. *Id.* at 478–79.

250. *Id.* at 485.

251. 497 F.2d 516, 522 (5th Cir. 1974).

interdependence may be demonstrated by the investors' collective reliance on the promoter's expertise," and that where such reliance is present, vertical commonality exists even if the promoter does not share in the profits of the venture.[252] In so holding, the court "recognize[d] that . . . the second and third prongs of the *Howey* test may in some cases overlap to a significant degree."[253]

The limitations of the vertical commonality tests are clearly apparent when applying this dated framework to the operation of The DAO. The SEC cast Slock.it and its founders as The DAO's promoters but failed to explain that these "promoters" were bound by the exact same terms as every other DAO token holder. Unlike in a traditional enterprise where the promoter or management enjoys special decision making privileges, access to information not available to investors, or the ability to control entity assets, here, as the promoter, Slock.it was just one of many token holders, holding the same rights as any other token holder in The DAO enterprise.[254] Neither Slock.it nor any other individual or entity could take any action to spend DAO resources, incur obligations, or take any other action independent of a vote of DAO token holders.[255] Thus, while it can be argued that there was a direct correlation between the success of the promoter and that of other DAO token holders, this correlation existed solely because the promoters were also token holders and not because other token holders were in any way dependent on any special skills or expertise of Slock.it.

The lack of a central authority to make decisions for The DAO made it impossible for token holders to have "collective reliance on the promoter's expertise."[256] Instead, all decisions regarding The DAO were made collectively by all token holders, demonstrating that, unlike in *Koscot*, this was not a "scheme[] in which promoters retain[ed] immediate control over the essential managerial conduct of an enterprise and where the investor's realization of profits [was] inextricably tied to the success of the promotional scheme."[257] The only way that DAO token holders' success was intertwined with Slock.it's success was that both groups held DAO tokens—thus

252. Long v. Shultz Cattle Co., 881 F.2d 129, 141 (5th Cir. 1989).

253. *Id.*

254. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 1 (discussing how The DAO allows "participants [to] maintain direct real-time control of contributed funds," and puts in place "governance rules [that] are formalized, automated and enforced using software").

255. *See id.*

256. *Continental Commodities*, 497 F.2d at 522.

257. SEC v. Koscot Interplanetary, Inc., 497 F.2d 473, 485 (5th Cir. 1974).

essentially creating horizontal commonality.[258] But as detailed above, every individual token holder had the ability to opt out of funding any individual proposal, so it is impossible to say that any individual token holder's fortunes were dependent on or inextricably linked with the promoter's fortunes.[259] Having failed to satisfy any of the common enterprise tests, it seems clear that DAO tokens are not securities under *Howey*.

E. Expectation of Profits from the Efforts of Others

As originally articulated by the Supreme Court, the *Howey* test required that an investor be "led to expect profits *solely* from the efforts of the promoter or a third party."[260] However, over time the federal courts have weakened this requirement by reading out the word "solely" and instead holding that this prong of the *Howey* test is met where "the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise."[261]

The SEC concluded that "The DAO's investors relied on the managerial and entrepreneurial efforts of Slock.it and its co-founders, and The DAO's curators to manage The DAO and put forth project proposals that could generate profits for The DAO's investors."[262] Further, it concluded that DAO token holders' ability to vote on proposals was "a largely perfunctory one"[263] and therefore did not constitute the "essential managerial efforts without which the risk could not pay off."[264] I respectfully disagree.

The SEC went to considerable lengths to paint Slock.it, its cofounders, and DAO curators as the parties whose efforts were critical to the success of The DAO.[265] A closer examination of The DAO's structure and operation, however, undercuts this assertion. While the SEC is correct that Slock.it and its cofounders devoted significant time and resources to promoting The DAO, it ignored the

---

258. *See supra* notes 36–39.

259. *See* JENTZSCH WHITE PAPER, *supra* note 2, at 2 ("If an individual, or a group of token holders, disagree with a proposal and want to retrieve their portion of the ether before the proposal gets executed, they can submit and approve a special type of proposal to form a new DAO.").

260. SEC v. W.J. Howey Co., 328 U.S. 293, 299 (1946) (emphasis added).

261. SEC v. Glenn W. Turner Enters., 474 F.2d 476, 482 (9th Cir. 1973).

262. SEC REPORT, *supra* note 18, at 12.

263. *Id.* at 14.

264. *Id.* at 13–14.

265. *Id.* at 12–14.

fact that once The DAO smart contract was launched on the Ethereum platform, neither they nor any other individual or entity controlled it.[266] The SEC concluded that Slock.it and its cofounders "held themselves out to investors as experts in Ethereum . . . and told investors that they had selected persons to serve as Curators based on their expertise and credentials."[267] Again, while technically true, these statements are pregnant with the implication that somehow Slock.it or the curators exercised some special control over The DAO's actions—an assertion that is patently and provably untrue.

The SEC's view of both the role of curators and the token holders' ability to control the enterprise through voting stands in stark contrast to the actual operation of The DAO as described in Jentzsch's white paper and the materials used by Slock.it to promote The DAO—the same materials that the SEC ostensibly relied on in compiling its report.[268] A review of these and other sources directly contradicts the conclusion that the curators' whitelisting of proposals served as some sort of merit review upon which DAO token holders depended.[269] Contrary to the SEC's framing, the role of the curators was not to provide any sort of merit review, determine the order of proposals, or to provide any sort of endorsement or seal of approval on proposals.[270] Prior to The DAO's launch, Stephan Tual, cofounder and COO of Slock.it made this clear:

> Curators curate the whitelist, the list of Contractors authorized to receive ether from the DAO. A Curator therefore holds two primary functions:
>
> • First, when a DAO Token Holder submits a Proposal in the form of a smart contract, the Curator checks that the published Contract on the Ethereum blockchain matches the

---

266. *See The DAO Wishes Gav All The Best*, DAOHUB (May 13, 2016), https://blog.daohub.org/the-dao-wishes-gav-all-the-best-c678f65a6f5f ("Curators have their role, but they are not responsible for the DAO's future: each and every DAO Token Holder is. . . . By design, The DAO's code and the DAO Token Holders are what is running the show.").

267. SEC REPORT, *supra* note 18, at 12.

268. *Id.* at 3–5 nn.7–19, 7 n.22, 9 nn.28–31 & 33.

269. *Id.* at 12–13 ("The expertise of The DAO's creators and Curators was critical in monitoring the operation of The DAO, safeguarding investor funds, and determining whether proposed contracts should be put for a vote. Investors had little choice but to rely on their expertise.").

270. Stephan Tual, *On DAO Contractors and Curators*, MEDIUM: SLOCK.IT BLOG (Apr. 9, 2016), https://blog.slock.it/on-contractors-and-curators-2fb9238b2553.

source code the Contractor claims to have deployed (this is done by comparing bytecode).

- Second, a Curator confirms that a Proposal comes from an identified person or organization. This is done by asking the entity submitting the Proposal to send a signed transaction with a certain set of data only known to the Curator and the author of the Proposal, thereby confirming the author of the Proposal.

The above are the only two functions of a Curator. For clarity, the following tasks are therefore *not* the role of a Curator, but instead the role of the DAO as a whole:

- Evaluate whether a Proposal is 'good' or not.
- Audit the Proposal's smart contract code.
- Provide legal advice regarding the Proposal (if any).
- Take responsibility for the Proposal.[271]

Other sources confirm the limited role of DAO curators, including a blog post by one of the original DAO curators, Dr. Gavin Wood, who described his role as "purely . . . a means of identity-verification" and stated that "[t]he role of the 'curators' in [S]lock.it's DAO design is trivial and entirely algorithmic—*no judgment whatsoever is required*."[272] The DAO's own website, relied upon by the SEC for other factual assertions contained in its report,[273] goes to great lengths to make clear that DAO curators do not exercise special powers within The DAO and are not responsible for the content of proposals or for any type of merit review:

It is worth being explicit: Curators are not responsible for providing advice (legal or otherwise) or taking responsibility

---

271. *Id.* To the extent that one questions whether assertions made by Slock.it on its own blog are true, it is worth noting that the SEC used this same blog as the source for other factual assertions in its Report. *See* SEC REPORT, *supra* note 18, at 5 nn.17 & 19, 9 nn.28, 30 & 33.

272. Gav Would, *Why I've Resigned as a Curator of the DAO*, MEDIUM (May 13, 2016), https://medium.com/@gavofyork/why-ive-resigned-as-a-curator-of-the-dao-238528fbd447.

273. *See* SEC REPORT, *supra* note 18, at 5 & n.18.

> for any proposal. Curators are neither the builders nor the founders of The DAO. The responsibility of The DAO's success falls on the Contractors to make good proposals and the DAO Token Holders to evaluate, debate, and vote on those proposals. Curators have their role, but they are not responsible for the DAO's future: each and every DAO Token Holder is.[274]

Every DAO token holder had equal rights, power, and access to information, much like in a general partnership. Thus, examining cases where courts have addressed whether investors in a general partnership relied on the efforts of others is informative here. The key line of cases in this area begins with the Fifth Circuit's 1981 decision in *Williamson v. Tucker*.[275] The *Williamson* court held that "[a]lthough general partners and joint venturers may not individually have decisive control over major decisions, they do have the sort of influence which generally provides them with access to important information and protection against dependence on others."[276] The *Williamson* court recognized that while "the courts that have ruled on the issue have held that a general partnership or joint venture interest generally cannot be an investment contract under the federal securities acts,"[277] there may be narrow factual situations that would bring such interests within the "reach of the federal securities laws."[278] Thus, the court devised a three factor test for when partnership interests constitute securities:

> A general partnership or joint venture interest can be designated a security if the investor can establish, for example, that (1) an agreement among the parties leaves so little power in the hands of the partner or venturer that the arrangement in fact distributes power as would a limited partnership; or (2) the partner or venturer is so inexperienced and unknowledgeable in business affairs that he is incapable of intelligently exercising his partnership or venture powers; or (3) the partner or venturer is so dependent on some unique entrepreneurial or managerial ability of the promoter or manager that he cannot replace the manager of the enterprise

---

274. *See The DAO Wishes Gav All The Best*, *supra* note 266.
275. 645 F.2d 404 (5th Cir. 1981).
276. *Id.* at 422.
277. *Id.* at 421.
278. *Id.* at 422.

> or otherwise exercise meaningful partnership or venture powers.[279]

Satisfying any one of the three *Williamson* factors renders an investment contract a security.[280] Under the *Williamson* test, "the focus is on investors' expectations when they originally invest, not 'what actually transpires after the investment is made, i.e., whether the investor later decides to be passive or to delegate all powers and duties to a promoter or managing partner.'"[281]

In evaluating the first *Williamson* factor, courts look to the partnership agreement or other formal documents to determine if the "agreement among the parties leaves so little power in the hands of the partner or venturer that the arrangement in fact distributes power as would a limited partnership."[282] In *Schooler*, the SEC argued that investors lacked power in the partnership due to the sheer number of partners.[283] Rejecting this contention, the court held that "the number of investors in a general partnership has little to do with the formal powers that are given to investors in the partnership documents" and that there is no "rigid rule with respect to partnership numbers."[284] Instead, the court concluded that "[i]t is clear in the case law that, with respect to the first *Williamson* factor, what courts look for is a partnership agreement that plainly gives the promoter or manager a power advantage over the investors."[285] Moreover, courts have held that "the first factor is addressed to the legal powers afforded the investor by the formal documents without regard to the practical impossibility of the investors invoking them."[286]

A review of the documents underpinning investment in The DAO—Jentzsch's white paper, as well as the materials promoted by Slock.it prior to The DAO's launch—confirms that all DAO

---

279. *Id.* at 424.

280. SEC v. Schooler, 902 F. Supp. 2d 1341, 1348 (S.D. Cal. 2012) ("The presence of any *one Williamson* factor renders an investment contract a security." (citing SEC v. Merch. Capital, LLC, 483 F.3d 747, 755 (11th Cir. 2007))).

281. *Id.* at 1347 (quoting Koch v. Hankins, 928 F.2d 1471, 1477 (9th Cir. 1991); *see also Merchant Capital*, 483 F.3d at 756 ("We analyze the expectations of control at the time the investment is sold, rather than at some later time after the expectations of control have developed or evolved.").

282. *Schooler*, 902 F. Supp. 2d at 1348 (quoting *Williamson*, 645 F.2d at 424).

283. *Id.*

284. *Id.*

285. *Id.* at 1349.

286. *Koch*, 928 F.2d at 1478.

token holders, including the promoters, had equal voting rights.[287] This structure, where no individual or group of individuals had any powers within the enterprise that were not held by all token holders, demonstrates the problem with applying a legal framework developed for centralized institutions to a decentralized entity like The DAO. The analysis is built on the idea that, by depriving investors of critical information, a manager or management committee can exercise superior power within the enterprise at the expense of the investors.[288] But because The DAO lacked any central manager or committee, the rationale of the case law does not hold. Conceptually, The DAO was a general partnership where every single decision was made not by a management or executive committee but by a vote of all token holders. All token holders had the same rights and powers; thus, it cannot be said that "the arrangement . . . distribute[d] power as would a limited partnership," where general partners may be empowered to marginalize limited partners.[289]

The SEC concluded that DAO token holders were dependent on the efforts of others because there was no "mechanism to provide DAO Token holders with sufficient information to permit them to make informed voting decisions" and that "based on . . . the few draft proposals discussed in online forums, there [were] indications that contract proposals would not have necessarily provide[d] enough information for investors to make an informed voting decision."[290] The SEC also concluded that "the pseudonymity and dispersion of DAO Token holders made it difficult for them to join together," thus preventing them from asserting real power in the enterprise.[291] These two assertions suffer the same flaw—they assume that there was some promoter or manager who gained power (or deprived the investors of power) by not sharing this information.[292] That was simply not the case. The fact that the information contained in contract proposals was,

---

287. *See The DAO Wishes Gav All The Best*, *supra* note 266.

288. *See* SEC v. Arcturus Corp., 171 F. Supp. 3d 512, 525 (N.D. Tex. 2016) (concluding that investors lacked power because managing venturer withheld critical information).

289. Williamson v. Tucker, 645 F.2d 404, 424 (5th Cir. 1981).

290. SEC REPORT, *supra* note 18, at 14.

291. *Id.*

292. *Contra Arcturus Corp.*, 171 F. Supp. 3d at 525 (holding that individual venturers' "right to vote or call a meeting . . . was absolutely hindered by the inability of the venturers to contact each other," because the managing venturer actively guarded and refused to disclose this information).

in the SEC's view, insufficient to make an informed investment decision does not explain how DAO token holders were dependent on others when there was no manager or committee who had access to this supposedly missing information. Nor does the SEC's conclusion as to the pseudonymity and dispersion of DAO token holders demonstrate that token holders were dependent on others because, again, there were no "others" who had this information.

The second and third *Williamson* factors both concern investors' reliance on the promoter or manager. Under the second *Williamson* factor, "the relevant inquiry is whether 'the partner or venturer is so inexperienced and unknowledgeable *in business affairs* that he is incapable of intelligently exercising his partnership or venture powers.'"[293] To satisfy this factor, the investors must be so inexperienced and unknowledgeable that "they would be relying solely on the efforts of the promoters to obtain their profits."[294] Similarly, the third factor looks to "whether 'the partner or venturer is so dependent on some unique entrepreneurial or managerial ability of the promoter or manager that he cannot replace the manager of the enterprise or otherwise exercise meaningful partnership or venture powers.'"[295]

Unsurprisingly, the SEC did not discuss or even address the knowledge and experience held by DAO token holders. But based on the marketing efforts used and the relative complexity of purchasing DAO tokens, it seems highly unlikely that DAO token holders were so inexperienced and unknowledgeable about the Ethereum platform and decentralized applications that they were dependent on the efforts of others. DAO tokens were marketed by Slock.it through its website, blog, and white paper—resources read not by the general public but by those deeply involved in the development of the Ethereum platform.[296] More fundamentally, this test again illustrates the problem with applying existing legal frameworks to decentralized organizations—assuming that DAO token holders lacked the requisite experience and knowledge so as to make them dependent, who were they dependent upon? The SEC concluded that token holders were dependent on DAO curators,[297] but as discussed above, the role of curators was

---

293. Koch v. Hankins, 928 F.2d 1471, 1479 (9th Cir. 1991) (quoting *Williamson*, 645 F.2d at 424).

294. SEC v. Merch. Capital, LLC, 483 F.3d 747, 762 (11th Cir. 2007).

295. *Koch*, 928 F.2d at 1479 (quoting *Williamson*, 645 F.2d at 424).

296. *See supra* text accompanying notes 265–67.

297. *See* SEC REPORT, *supra* note 18, at 12–15.

limited to whitelisting proposals. Curators had no ability to bind The DAO, spend The DAO's resources, or take any other organizational action without a vote of token holders.[298]

Even if one views curators as enjoying some special management prerogatives within The DAO enterprise, because curators could be removed by token holders for any reason and at any time, it cannot be said that token holders were dependent on the curators. In *Goodwin v. Elkins & Co.*, the Third Circuit addressed a similar situation in a partnership agreement where a partner claimed he was dependent on the executive committee and managing partner who oversaw the business.[299] In rejecting the partner's contention, the court held that because the partner was entitled to "participate in the nomination, election, or removal of the Executive Committee and the Managing Partner," he "had a substantial role in the management of the firm," and therefore could not claim he was dependent on the efforts of others.[300] Applying the same rule here, not only were DAO token holders able to appoint and terminate curators, but unlike the executive committee in *Goodwin* that actually made decisions for the enterprise, DAO curators were limited to whitelisting proposals, which then still had to be voted on by DAO token holders. In short, curators had no ability to invest, spend, or otherwise put The DAO resources at risk without a majority vote of token holders.

With the actual operation of The DAO put in its proper factual context, it becomes clear that the SEC's conclusion that Slock.it and the curators provided "essential managerial efforts which affect the failure or success of the enterprise" is, at best, questionable.[301] While the curators were responsible for verifying the identity of contractors and ensuring that smart contracts posted on the Ethereum blockchain matched the source code that contractors claimed to have deployed, neither of those actions created the type of dependency necessary to satisfy the *Howey* test. All decision-making control was vested exclusively in DAO token holders who had to vote to approve any proposal and thereby retained complete control over the actions of The DAO. Moreover, because DAO token holders retained the power to appoint and remove curators for any reason via a majority vote, it can hardly be said that the token holders had "no reasonable alternative to

298. *See supra* text accompanying notes 256–57.

299. 730 F.2d 99, 104–05 (3d Cir. 1984).

300. *Id.* at 105.

301. SEC v. Glenn W. Turner Enters., 474 F.2d 476, 482 (9th Cir. 1973).

reliance on [the curators]," a prerequisite to satisfying *Howey*'s third prong.[302] As former curator Dr. Gavin Wood said,

> "It sounds rather stupid to point out so bluntly, but the two critical properties concerning a DAO is that it is decentralized and that it is autonomous. *As such it acts for itself; no individual, nor group of individuals have any authority over the organization over and above the aggregated shareholders.*"[303]

IV. POST-DAO REPORT DEVELOPMENTS

Interestingly, the SEC's questionable *Howey* analysis has been widely accepted without criticism.[304] This likely has occurred for several reasons. First, there simply are not many attorneys working in the blockchain space, and thus there is not a deep pool of knowledge as to how this technology operates and intersects with the law. Second, lawyers have a tendency to reflexively place new technology into old legal frameworks—whether such a framework is appropriate or not. You can see this in the SEC's concerted effort to frame Slock.it, its cofounders, and the DAO curators as in control of The DAO, despite the abundance of evidence indicating that this was not in fact true. Third, for many practicing attorneys it really does not matter if the SEC presented a flawed analysis because it is the only guidance in

---

302. *Goodwin*, 730 F.2d at 109 (quoting Williamson v. Tucker, 645 F.2d 404, 422 (5th Cir. 1981)); *see also* SEC REPORT, *supra* note 18, at 12–15.

303. Would, *supra* note 272 (emphasis added).

304. *See, e.g.*, Brian Patrick Eha, *SEC Report May Put an End to ICO Boom*, AM. BANKER (July 25, 2017, 7:49 PM), https://www.americanbanker.com/news/sec-report-may-put-an-end-to-ico-boom; Gil Penchina, *SEC Shows Support for ICOs that Are Not Obviously Securities*, TECHCRUNCH, https://techcrunch.com/2017/09/14/sec-shows-support-for-icos-that-are-not-obviously-securities/ (last visited Nov. 8, 2018) (discussing The DAO and Protostarr ICOs and concluding that "[i]n both cases, even a non-lawyer can see that both were clearly securitization and under the SEC's jurisdiction"); Jeff John Roberts, *The SEC's Big Digital Coin Ruling: What It Means*, FORTUNE (July 26, 2017), http://fortune.com/2017/07/26/sec-icos/; Katie Roof, *SEC Regulators Are Coming After ICOs*, TECHCRUNCH, https://techcrunch.com/2017/07/25/sec-regulators-are-coming-after-icos/ (last visited Nov. 8, 2018); Avi Salzman, *The SEC May Have Just Popped the Digital Coin Bubble*, BARRONS (July 25, 2017, 6:25 PM), http://www.barrons.com/articles/the-sec-may-have-just-popped-the-digital-coin-bubble-1501021510 ("The SEC released an investigative report on Tuesday that is likely to pop a growing bubble in digital coins . . . .").

this area and thus, must be relied on in advising clients. To do otherwise would be malpractice.

It would be easy to think that perhaps the SEC just whiffed on this one—that it did not understand the technology or how it worked. But the SEC is filled with intelligent and competent lawyers who attended the best law schools and worked at the most elite white shoe law firms across the country. Moreover, the SEC wields substantial investigatory resources, access to experts and academics, and the full might of the U.S. government. It seems highly unlikely that this was a random errant analysis and instead far more likely that SEC officials made a calculated decision to use the report on The DAO to send a strong and direct message to the larger ICO marketplace: we are watching, and we do believe that we have enforcement power in this space. Neither the fact that The DAO was structured and operated differently from most blockchain companies nor the fact that DAO tokens fail the *Howey* test could overcome the government's desire to assert itself in this space before the ICO industry grew too large to control.[305]

With ICOs suddenly raising large amounts of money, including multiple individual offerings raising in excess of $100 million,[306] the SEC likely believed that it needed to send a message to would-be fraudsters that this was no longer the lawless digital Wild West. But by presenting a slanted and unsupportable analysis, the SEC's report on The DAO instead demonstrates the problems inherent in rushing to regulate new technological innovations with tools built in and for the twentieth century. Perhaps more troubling, as discussed below, the SEC's strategy of regulation through enforcement actions is likely

---

305. The idea that a central government would attempt to tamp down the coming widespread adoption of crypto-assets in the name of self-preservation is not at all far-fetched. The free flow of value that circumvents central governmental authority by avoiding fiat currency, combined with the global reach of these crypto-assets, represents a potential threat to the control exercised by central governments and banks. A world where individuals no longer must rely on fiat currency issued by central banks is a world where the power of central governments is significantly diminished. While conspiracy theories have long circulated regarding the U.S. government's fear of bitcoin and other cryptocurrencies, this idea has some merit and should be discussed seriously by lawyers and legal scholars. The more the general public embraces cryptocurrencies that, unlike fiat currencies, cannot be manipulated by central governments, the less power governments have over monetary policy, and thus, the less power they have over the economy as a whole. While I do not believe that we are anywhere close to reaching this tipping point, the idea of widespread adoption of cryptocurrencies represents an existential threat to centralized governments the world over.

306. *See supra* notes 9–12 and accompanying text.

to prove ineffective in curbing the significant amount of fraud that has emerged in the ICO marketplace.

A. The Move to "Utility Tokens"

One result of the SEC's report has been a deluge of articles drawing a distinction between so-called equity tokens, like those the SEC contends The DAO issued, and so-called "utility" tokens.[307] Utility tokens are promoted not as equity investments but essentially as pre-paid coupons that will unlock value in yet-to-be-built software programs or platforms.[308] The majority of ICOs occurring right now are marketing and selling what they describe as utility tokens.[309] In theory, purchasers buy these tokens so that they can later use them within the issuing entity's distributed software ecosystem.[310] As the software ecosystem grows and develops, the number of users increases, driving up demand and with it the value of the tokens.[311] The majority of ICOs cap the number of crypto-tokens that will be issued, thereby ensuring that the value of the limited quantity of entity-specific crypto-tokens in circulation will increase as the issuing entity becomes more successful and garners more users.[312]

That utility tokens may have some functional utility within the issuing entity's ecosystem (assuming that the software ecosystem is actually built) leads to an interesting—and important for the

---

307. *See, e.g.*, Micha Benoliel, *Understanding the Difference Between Coins, Utility Tokens and Tokenized Securities*, MEDIUM (Aug. 8, 2017), https://medium.com/startup-grind/understanding-the-difference-between-coins-utility-tokens-and-tokenized-securities-a6522655fb91; Roberts, *supra* note 304; Shin, *supra* note 156; Josiah Wilmoth, *The Difference Between Utility Tokens and Equity Tokens*, STRATEGIC COIN, http://strategiccoin.com/difference-utility-tokens-equity-tokens (last visited Nov. 8, 2018).

308. *See* Wilmoth, *supra* note 307.

309. *See, e.g.*, ATLANT, TERMS OF TOKEN SALE 1–2 (2017) (on file with author); GLUON, GLU TOKEN TERMS OF TOKEN SALE 14–17 (2017) (on file with author); GRAFT NETWORK, PRE-SALE TERMS AND CONDITIONS 4, 12–15 (2017) (on file with author); INSTACOIN, TERMS OF TOKEN SALE 8–12 (2017) (on file with author); KIK, TERMS OF USE AGREEMENT 8–9 (2017) (on file with author).

310. *See* Shin, *supra* note 13, at 66 ("Since most of these platforms cap the number of tokens, increased usage jacks up the demand for them and should, in turn, boost the price.").

311. Steve McKie, *Understanding the Ethereum ICO Token Hype*, MEDIUM: BLOCKCHANNEL (June 14, 2017), https://medium.com/blockchannel/understanding-the-ethereum-ico-token-hype-429481278f45; Jeff John Roberts, *Why Tech Investors Love ICOs—and Lawyers Don't*, FORTUNE (June 26, 2017), http://fortune.com/2017/06/26/ico-initial-coin-offering-investing/.

312. *See, e.g.*, Shin, *supra* note 156.

purposes of U.S. securities law—question: are these tokens essentially pre-paid coupons that may gain value based on the liquid market for the underlying service, or do crypto-tokens gain value based on the efforts of those building the underlying software ecosystem? Although many issuers are currently seeking to circumvent securities regulation by labeling their issuances as utility tokens, there is no legal basis upon which to think that such tokens, by mere virtue of their potential future utility, will not gain value based on the efforts of the promoters and therefore be considered securities under the *Howey* test. Moreover, in reality, at least at this early stage, the value of many crypto-tokens is being driven by speculative trading.[313] This high trading volume and the accompanying volatility of many of these crypto-tokens raises the potential for fraud and bolsters the argument that they should be regulated like traditional securities.

That said, the SEC's rambling entry into the ICO marketplace poses a threat to ICOs' promise of increased democratization—both of investment opportunities (away from accredited investors and towards open accessibility) and of opportunities for entrepreneurs who lack access to angel investors, venture capital, and the traditional capital markets.[314] The Ethereum platform is a global system, with innovators around the world developing and deploying decentralized applications.[315] As is true with any insertion of governmental regulation, those adverse to the costs of compliance will move from locations where that cost is high to where it is low.[316] Practically, that means that heavy-handed regulation by the U.S. government has the potential to lead to an exodus of innovation to other countries around the world that lack such significant regulatory structures.[317] Likewise, locking out U.S. residents from investing in ICOs puts

313. *See* Shin, *supra* note 13.

314. *See* Eha, *supra* note 304 ("The consequences could be devastating for the market in these new digital assets, should exchanges choose to bar American users or drop some tokens altogether instead of complying with U.S. securities laws.").

315. *See id.*

316. *See id.* ("Token sales are a global phenomenon, and the SEC alone cannot stop the trend. But the U.S. is the world's deepest pool of capital, and by late Wednesday afternoon the SEC's report was sending shock waves through social media."); *see also* Penchina, *supra* note 304 (discussing how post-SEC report on The DAO, the "LAToken postponed opening for the US such innovation as tokenized stocks and commodities which are currently tradable on the platform in other regions").

317. *See* Sujha Sundararajan, *ECB President: Bitcoin Not 'Mature' Enough to Be Regulated*, COINDESK (Oct. 20, 2017, 13:30 UTC), https://www.coindesk.com/ecb-president-bitcoin-not-mature-enough-to-be-regulated/ ("Mario Draghi, president of the European Central Bank (ECB), has said that cryptocurrencies are not 'mature' enough to be regulated.").

Americans at a disadvantage in what is one of the fastest growing segments of the capital markets.[318]

The number of fraudulent ICOs have proliferated in the past year, and the SEC's regulation-through-enforcement-actions strategy has done little to abate this trend. By choosing to view this burgeoning marketplace through the traditional securities law framework, the SEC may have slowed down the ICO trend, but its failure to provide for any certainty in the ICO marketplace—either through a clear and generally applicable regulatory analysis or the announcement of a specific regulatory safe harbor—has done little to actually rid the space of fraud, and instead is likely, in the long term, to stifle innovation and investment.[319] While the SEC has been aggressive in going after fraudulent offerings, the sheer number of such scams has proliferated, making regulation through enforcement an ineffective tool in stemming the tide of ICO scams.

B. SEC's Early Enforcement Actions Against Token Issuers

Since issuing its report on The DAO, the SEC has been active in pursuing enforcement actions against token issuers.[320] To date, nearly all of these enforcement actions have been brought against individuals or entities engaged in clearly fraudulent ICOs.[321] In September 2017, the SEC filed a complaint against RECoin and its founders, alleging that the company defrauded investors through two separate ICOs that purported to issue digital tokens backed by investments in real estate and diamonds.[322] In reality, there was not only no real estate or diamonds backing the tokens, but the tokens themselves were never created or provided to investors.[323] In short,

---

318. *See* Jen Wieczner, *Cryptocurrency ICOs Are Making Bitcoin Startups Richer than VCs Ever Did*, FORTUNE (July 28, 2017), http://fortune.com/2017/07/28/bitcoin-cryptocurrency-ico/ ("ICOs have now raised nearly four times as much money as bitcoin companies raised in venture capital dollars so far this year. . . . And that's at a time when venture capital is booming among blockchain companies.").

319. *See supra* note 317.

320. *See generally Initial Coin Offerings (ICOs)*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/ICO (last visited Nov. 8, 2018).

321. *See id.*

322. *See* U.S. SEC. & EXCH. COMM'N, SEC EXPOSES TWO INITIAL COIN OFFERINGS PURPORTEDLY BACKED BY REAL ESTATE AND DIAMONDS (2017), https://www.sec.gov/news/press-release/2017-185-0 (detailing enforcement action against individual and company whose fraudulent ICO raised $300,000).

323. Complaint at 11, SEC v. RECoin Grp. Found., LLC, 1:17-cv-05725-RJD-RER (E.D.N.Y. Sept. 29, 2017) ("[C]ontrary to Zaslavskiy's and REcoin's misstatements about the nature of the offering in the REcoin ICO, investors who transferred funds to

RECoin was a flat out scam—there was no actual company, nor were there any assets or other business operations that had the potential to generate returns for token purchasers.[324]

In December 2017, the SEC filed a complaint against Dominic Lacroix, a Canadian man behind the sale of a token called PlexCoin.[325] The SEC described Lacroix as "a recidivist securities law violator in Canada" who had previously been enjoined from selling PlexCoins by a Quebec Tribunal.[326] The SEC's complaint alleged that, much like RECoin, PlexCoin was "nothing more than a fraudulent scam run primarily by Lacroix and his cohorts" and that "[t]here was no meaningful market maintenance and no meaningful project development."[327] Instead, "Lacroix actually used a portion of the proceeds to pay for personal expenses."[328]

This wave of enforcement actions continued into 2018. In January, the SEC filed a complaint against Dallas-based AriseBank, which allegedly "used social media, a celebrity endorsement, and other wide dissemination tactics to raise what it claims to be $600 million of its $1 billion goal in just two months."[329] The complaint alleged a brazen scheme to defraud investors, in which AriseBank "falsely stated that it purchased an FDIC-insured bank which enabled it to offer customers FDIC-insured accounts and that it also offered customers the ability to obtain an AriseBank-branded VISA card."[330] None of these claims by AriseBank were true.[331]

Later in the spring of 2018, the SEC filed complaints against two other issuers, Centra Tech Inc. and Titanium Blockchain Infrastructure Services, Inc.[332] Both offerings were allegedly scams

---

Zaslavskiy via the REcoin website never received any form of digital asset, token, or coin, and no token or coin for REcoin has ever been developed.").

324. *See generally id.*

325. *See* U.S. SEC. & EXCH. COMM'N, SEC HALTS ALLEGED INITIAL COIN OFFERING SCAM (2018), https://www.sec.gov/news/press-release/2018-8.

326. Complaint at 1–2, SEC v. PlexCorps, 1:17-cv-07007-CBA-RML (E.D.N.Y. Dec. 1, 2017).

327. *Id.* at 21.

328. *Id.*

329. *See* U.S. SEC. & EXCH. COMM'N, *supra* note 325.

330. *Id.*

331. *Id.*

332. *See* U.S. SEC. & EXCH. COMM'N, SEC HALTS FRAUDULENT SCHEME INVOLVING UNREGISTERED ICO (2018), https://www.sec.gov/news/press-release/2018-53; U.S. SEC. & EXCH. COMM'N, SEC OBTAINS EMERGENCY ORDER HALTING FRAUDULENT COIN OFFERING SCHEME (2018), https://www.sec.gov/news/press-release/2018-94.

that materially misled investors into purchasing worthless tokens.[333] The SEC's early enforcement actions against token issuers, while necessary and effective, have primarily targeted blatant frauds.[334] AriseBank, PlexCoin, Centra Tech, and Titanium Blockchain all represent low hanging fruit—offerings designed and perpetrated as scams, not true fund raises for actual development of products or companies. While these actions are beneficial, such reactionary efforts are unlikely to prevent ongoing fraud in the space.

The SEC is currently playing a game of whack-a-mole in which it is overwhelmingly outmatched. A recent study by the blockchain firm Satis Group concluded that "approximately 78% of ICOs were Identified Scams."[335] With over 1,500 crypto-assets now in existence,[336] the scale of the problem dramatically dwarfs the SEC's capacity to regulate through enforcement actions. For every successful enforcement action, many other fraudulent token offerors are successful in bilking investors looking for the next get-rich-quick scheme.

---

333. *See supra* note 332.

334. *Cf.* Pete Schroeder & Michelle Price, *SEC Halts Virtual Coin Offering, Issues Investor Warning*, REUTERS (Dec. 11, 2017, 1:37 PM), https://www.reuters.com/article/us-munchee-ico/sec-halts-virtual-coin-offering-issues-investor-warning-idUSKBN1E52CR ("Monday's enforcement action [against Munchee Inc] was significant because it showed SEC would step in to address ICOs for registration violations even if there were no claims of fraud, according to SEC officials.").

335. *See* DOWLAT, *supra* note 8, at 23 (defining "Identified Scams" as "[a]ny project that expressed availability of ICO investment (through a website publishing, ANN thread, or social media posting with a contribution address), did not have . . . [an] intention of fulfilling project development duties with the funds, and/or was deemed by the community (message boards, website or other online information) to be a scam").

336. *Id.* at 1.

V. RETHINKING THE REGULATORY FRAMEWORK

A. The SEC's Limited Enforcement Ability

If the potential harm to innovation and investment opportunities and the sheer number of fraudulent offerings are not enough reason to rethink the current regulatory approach to ICOs, the enforcement challenges presented by public blockchains provide an even greater argument for a new regulatory paradigm. By its own admission, the SEC likely faces considerable hurdles in enforcing U.S. securities laws against global blockchain entities.[337] The SEC's July 25, 2017 Investor Bulletin explicitly states that "[l]aw enforcement officials may face particular challenges when investigating ICOs and, as a result, investor remedies may be limited."[338] The bulletin goes on to detail the investigative and enforcement challenges unique to ICOs, including the difficulty of tracing money due to the lack of traditional financial institutions, the international scope of ICOs and restrictions on the SEC's ability to obtain and use information from abroad, the lack of any central authority on the blockchain, and the U.S. government's inability to freeze or secure investor funds held in cryptocurrencies.[339] While the FBI and other law enforcement agencies have increasingly found ways to track cryptocurrencies and crack the pseudonymity of actors on the blockchain, such investigative work is both expensive and time consuming and therefore not likely to be deployed broadly to police the ICO marketplace.[340] Thus, while

---

337. *See Investor Bulletin: Initial Coin Offerings*, *supra* note 18.

338. *Id.*

339. *Id.*

340. *See* Kyle Torpey, *Former SEC Attorney Explains Which ICOs Will Be Targeted with Regulatory Action*, FORBES (Aug. 31, 2017, 3:09 PM), https://www.forbes.com/sites/ktorpey/2017/08/31/former-sec-attorney-explains-which-icos-will-be-targeted-with-regulatory-action/#22ff9719b4b0 (quoting former SEC Enforcement Division attorney Nick Morgan: "They will be looking to deploy their resources efficiently, and that's why I say I think the next case they're going to bring will involve fraud because they can't possibly go after all the purveyors of ICOs—they just don't have the resources to do that."); *see also* FED. BUREAU OF INVESTIGATION, *supra* note 135 (discussing bitcoin and the "unique complexities for investigators because of its decentralized nature," but concluding with "medium confidence that law enforcement can identify, or discover more information about malicious actors if the actors convert their bitcoins into fiat currency"); MURPHY, MURPHY & SEITZINGER, *supra* note 135 ("Because of the public ledger, researchers have found that, using sophisticated computer analysis, transactions involving large quantities of Bitcoin can be tracked and claim that if paired with current law enforcement tools it would be possible to gain a lot of information on the persons moving the Bitcoins.").

the SEC will likely continue to bring enforcement actions against low-level fraudsters who advertise outside the blockchain and utilize public exchanges to move their ill-gotten gains from cryptocurrencies to fiat currencies,[341] it is unlikely that it will have much success shutting down those who deploy robust operational security in order to leverage the blockchain's pseudonymity.[342]

B. Endogenous Regulation as a Path Forward

Against the backdrop of these limitations, I propose a different path forward. Instead of attempting to fit this square peg into a round hole, perhaps it is time to step back and think about what safeguards we actually need in the ICO space and what the most effective mechanism is for putting such safeguards in place. At this early development stage, both sides, developers and sovereign governments alike, have incentive to work together to build a legal framework that provides safeguards against potential fraud while at the same time allows this developing technology the needed capital to grow. For their part, sovereign governments face serious challenges in enforcing securities laws in the blockchain world through top-down regulation.[343] Because the majority of ICOs are currently launched on the Ethereum platform, the SEC should encourage and work with Ethereum developers to integrate legal principles directly into the code that governs the platform. Likewise, Ethereum developers should capitalize on the widespread acceptance in the Ethereum community of the idea that "code is law" to build consensus around providing more robust legal protections within the platform's code.

This could be accomplished by both sides coming together to expressly endorse a safe harbor in which offering entities who satisfy specific requirements could issue crypto-tokens without registering with the SEC and with assurances that the SEC would not take enforcement action against them.[344] The SEC has made it clear that

---

341. *See* Torpey, *supra* note 340 ("Throughout the interview, [former SEC Enforcement Division attorney Nick] Morgan made the case that the SEC's next case involving an ICO would likely focus on fraudulent activity . . . .").

342. *Id.*

343. *See* Dewey & Emerson, *supra* note 123 ("Given the decentralized nature of distributed ledgers, the U.S. government is relatively helpless to end the practice, except for those operating inside the United States or jurisdictions with U.S. friendly extradition treaties.").

344. The safe harbor would apply only to utility tokens—that is tokens that provide some utility in the issuing entity's software system or platform and meet other requirements. This does nothing to prevent the issuance of equity tokens by companies

it intends to assert its regulatory muscle in this burgeoning space, but it faces real challenges in enforcement.[345] Likewise, many in the larger blockchain space have become skeptical of the ICO market, believing that it is rife with pump-and-dump schemes and other frauds.[346] This recognition, on both sides, of the need to police the ICO space provides an opening for a collaborative effort through which the SEC could fulfill its investor protection role and the Ethereum developer community could enhance the safety and reputation of the platform without direct governmental interference.

C. Creating a Safe Harbor Through Code as Law

Federal securities laws are based on the premise that investors can only make meaningful investment decisions if promoters are required to disclose the potential risks of investing in a given venture.[347] The SEC provides no merit reviews of registered offerings; instead, it mandates what information must be disclosed and ensures that such information is disclosed by reviewing registration statements.[348] There is no reason that a similar disclosure system could not be implemented directly on the blockchain. This could be done by building disclosure requirements into the crypto-token protocol itself, thereby fully animating code as law. While this mode of regulation looks radically different than what we are currently

---

who could either choose to register their offerings with the SEC or structure the offering to meet an enumerated exception.

345. *See* SEC REPORT, *supra* note 18, at 10; *see also* U.S. SEC. & EXCH. COMM'N, *supra* note 322 (detailing enforcement action against individual and company whose fraudulent ICO raised $300,000).

346. *See* Alyssa Hertig, *Ethereum to ICOs: You're Doing it Wrong*, COINDESK (Nov. 10, 2017, 9:00 UTC), https://www.coindesk.com/ethereum-icos-youre-wrong/ ("While many stakeholders in the cryptocurrency community believe the ICO space is fraught with bad actors, others more judiciously see it as all part of the learning process, with people trying to figure out just what ethereum and other blockchain technologies are (and aren't) capable of.").

347. *See* Monaghan, *supra* note 242, at 2141 (citing S. REP. NO. 73-47, at 1 (1933)) ("The aim is to prevent further exploitation of the public by the sale of unsound, fraudulent, and worthless securities through misrepresentation; to place adequate and true information before the investor; to protect honest enterprise, seeking capital by honest presentation, against the competition afforded by dishonest securities offered to the public through crooked promotion; to restore the confidence of the prospective investor in his ability to select sound securities; to bring into productive channels of industry and development capital which has grown timid to the point of hoarding; and to aid in providing employment and restoring buying and consuming power.").

348. *See id.*

accustomed to, it is technically feasible and likely the best option for providing true investor protection in the ICO space. Moreover, because there is already an established crypto-token protocol utilized by the majority of companies issuing tokens, additional safeguards that do not currently exist in the physical world could be integrated into ICOs.[349]

Broadly construed, an ICO safe harbor could provide issuers protection if the issued token (1) has utility in the software application or platform being developed, (2) does not provide equity in the issuing company, and (3) utilizes the universal ICO token protocol. By building investor safeguards into a universal ICO token protocol, issuers need not worry about compliance with U.S. securities laws—the code of the token itself would actuate the legal limitations, including (1) hard caps on the amount of cryptocurrency that can be exchanged in any given token offering, (2) lock-up periods that prevent token-holders from trading or exchanging tokens for a set period of time, (3) mandatory disclosure requirements to ensure identifiably liable parties, (4) binding arbitration agreements coupled with blockchain-based arbitration, and (5) a pooled risk-guarantee fund to provide recourse in cases of insolvency. Importantly, all of this could be built, implemented, and maintained completely on the Ethereum platform and without any direct intervention from sovereign governments.

Implementing a hard cap on the amount of ether or bitcoin that can be raised through an ICO, together with requiring token purchasers to hold their tokens for some minimal length of time, would help temper much of the wild speculation occurring today. The cap and lock-up period could be built into the universal ICO token protocol through code that automatically shuts down the offering once a predetermined amount of ether or bitcoin has been contributed to the issuing smart contract. Setting this hard cap at a relatively low

---

349. Currently, the majority of ICOs issued on the Ethereum platform utilize the ERC20 token protocol standard, which defines a specific set of commands that a token should implement, allowing developers to know exactly how a token will function within the larger Ethereum platform. *See* Amy Castor, *Ethereum 'Tokens' Are All the Rage. But What Are They Anyway?*, COINDESK (June 17, 2017), https://www.coindesk.com/ethereums-erc-20-tokens-rage-anyway/. The protocol "defines a set of six functions that other smart contracts within the [E]thereum ecosystem will understand and recognize." *Id.* This ensures that tokens issued under the protocol can interact with smart contracts on the Ethereum platform, as well as with virtually all wallets that support ether. *Id.* While to date this protocol has been used to ensure the interoperability of different crypto-tokens, there is no reason why specific investor safeguards could not also be coded into the ERC20 protocol. *Id.*

number, $5–10 million for example, would insure against massive investor losses and the governmental scrutiny that accompanies those losses. Likewise, a lock-up period coded into the smart contract could make the tokens un-tradable for a set period of time. Preventing token purchasers from immediately dumping their tokens would discourage speculative purchases by removing the immediate liquidity from these assets.

To provide more robust protection to investors, Ethereum core developers could build a decentralized autonomous organization that would require all token issuers to register and make certain disclosures. The universal ICO token protocol could require the filing of such registration via a smart contract. The registration smart contract itself would require the issuer to identify responsible parties for future liability purposes, include choice of law and forum selection clauses should litigation arise outside the blockchain platform, and make disclosures as to the risks involved in purchasing its tokens. Pairing such a registration system with a contractual provision requiring binding arbitration would provide token holders the ability to recoup losses not through reliance on sovereign judicial systems but instead, directly on the blockchain.

If an issuing entity went belly-up or an issuer engaged in fraud, token holders would first have recourse through binding arbitration on the blockchain. Numerous companies are already creating this infrastructure, including several arbitration platforms that are currently operational.[350] If a token holder is awarded damages through binding arbitration, the damages award could be automatically moved from the issuing entity's smart contract to the investor's wallet. If there are no funds in the issuing entity's smart contract, then the token holder could file a claim with the decentralized crypto-token registration organization to release information regarding the entity's finances and principals so that the token holder could pursue payment either through the blockchain or through a writ of garnishment or other collection method in a sovereign jurisdiction.

---

350. *See, e.g.*, *Decentralized Arbitration to Address Blockchain Disputes*, CRYPTOINSIDER, https://cryptoinsider.21mil.com/decentralized-arbitration-address-blockchain-disputes-jincor/ (last visited Nov. 8, 2018) (discussing a decentralized arbitration system for smart contract disputes); *World's First Smart Contract Based Arbitration Proceedings Conducted*, TRUSTNODES (July 17, 2017, 2:42 PM), http://www.trustnodes.com/2017/07/17/worlds-first-smart-contract-based-arbitration-proceedings-conducted (discussing a joint project by Intel, Siemens, Daimler and others that "claims to have conducted the world's first arbitration proceedings based on a smart contracts blockchain").

To further protect investors, the universal ICO token protocol could automatically sequester a percentage of funds raised through each ICO into a separate smart contract that serves as a pooled risk guarantee fund.[351] This smart contract would operate as a decentralized autonomous organization, with each contributing crypto-token issuer holding voting power. When a token holder is unable to collect an arbitration award directly from the entity or its principals, the token holder could file a claim with the pooled risk guarantee fund in much the same way that state insurance guarantee associations currently provide a backstop in the case of insurer insolvency. The smart contract at the heart of the guarantee fund could make automated payments when certain criteria are met and would provide a mechanism for complex claims to be approved through a vote of its token holders.

CONCLUSION

None of these proposals are fool-proof, and some of them likely face steep challenges to implementation. These potential prescriptions are put forward not as a cure-all but in an attempt to encourage lawyers and core development teams to work together in hopes of truly embracing code as law. The reality is that public blockchain platforms are built to be, and are in reality, extremely resistant to outside governmental interference or regulation. Thus, it is time to consider the somewhat radical proposition that blockchain platforms are less technological overlays to our existing economic, regulatory, and governmental systems and instead are independent sovereign jurisdictions that must develop their own legal structures, regulatory systems, and dispute resolution mechanisms. Viewing the blockchain through this lens opens up new possibilities for what regulation might look like in this space. If both sovereign governments and core development teams truly embrace the code as law paradigm, then the promised democratization of ICOs can actually be realized. In so doing, we can bring order to this new Digital Wild West, while at the same time nurturing these innovations that have the potential to truly disrupt the world.

---

351. This percentage need not be a fixed number but instead could be adjusted based on the amount of risk for each individual offering and the amount of risk in the marketplace as a whole.