COLUMBIA LAW REVIEW

VOL. 119 APRIL 2019 NO. 3

ARTICLES

COIN-OPERATED CAPITALISM

Shaanan Cohney, David Hoffman,***
*Jeremy Sklaroff*** & David Wishnick*****

This Article presents the legal literature's first detailed analysis of the inner workings of Initial Coin Offerings (ICOs). We characterize the ICO as an example of financial innovation, placing it in kinship with venture capital contracting, asset securitization, and (obviously) the IPO. We also take the form seriously as an example of technological innovation, in which promoters are beginning to effectuate their promises to investors through computer code, rather than traditional contract.

To understand the dynamics of this shift, we first collect contracts, "whitepapers," and other disclosures for the fifty top-grossing ICOs of 2017. We then analyze how the software code controlling the projects' ICOs reflected (or failed to reflect) their disclosures. Our inquiry reveals that many ICOs failed even to promise that they would protect investors against insider self-dealing. Fewer still manifested such promises in code. Surprisingly, in a community known for espousing a technolibertarian belief in the power of "trustless trust" built with carefully designed code, a significant fraction of issuers retained centralized control through

* P.h.D. Candidate, University of Pennsylvania, School of Engineering and Applied Science.

** Professor of Law, University of Pennsylvania Law School.

*** J.D. 2018, University of Pennsylvania Law School; M.B.A. 2018, The Wharton School of the University of Pennsylvania.

**** Academic Fellow, University of Pennsylvania Law School's Center for Technology, Innovation and Competition.

Author order is alphabetical. We thank Andrew Baker, Tom Baker, Robert Bartlett, Bill Bratton, Chris Brummer, Tony Casey, Peter Conti-Brown, Jill Fisch, Gabe Kaptchuk, Joshua Mitts, Mark Nevitt, Ori Oren, Max Raskin, Usha Rodrigues, Alec Webley, Kevin Werbach, and Aaron Wright for helpful comments. We further thank participants at the Third Annual Empirical Contracts Conference, the Institute for Law and Economics, Columbia University Law and Economics of Capital Markets Fellows and Contracts and Economic Organizations Workshops, Florida State, UCLA, FINRA Working Group, Canadian Law & Economics Association Annual Meeting, a Wharton Legal Studies & Business Ethics Department workshop, and faculty and fellows workshops at Penn Law for comments. We are also immensely grateful for our research assistant partners on this project: Alex Altieri, Joe Ebb, Kathryn Gardner, Amanda Gould, Taylor Hertzler, Jeffrey Luther, Rachel Mann, Matt Minsky, Hafidzi Razali, and Adam Zuckerman.

previously undisclosed code permitting modification of the entities' governing structures.

These findings offer valuable lessons to legal scholars, economists, and policymakers about the roles played by gatekeepers, the value of regulation, and the possibilities for socially valuable private ordering in a relatively anonymous, decentralized environment.

INTRODUCTION

If you believe what you read on social media, the world of venture finance is undergoing a sea change. Old institutions like banks and venture capital firms are finding themselves supplanted by masses of individuals coordinating through new financial platforms.[1] Excessively compensated elites are on the outs. They are being replaced—so say the believers—by equity crowdfunding, peer-to-peer lending, and the wisdom of the crowd.[2] The rise of the Initial Coin Offering (ICO) is a chapter in this story, and this Article's subject.[3]

Obviously, the ICO was named after the IPO, or "Initial Public Offering." But though the IPO has been familiar for almost a century, the ICO is exotic. Unlike its namesake, an ICO does not typically involve the sale of equity in (or governance rights pertaining to) a corporation.[4] Instead, ICO participants buy an asset—a "token"—that enables its holder to use or govern a network that the promoters plan to develop with the funds raised through the sale.[5] It would be as if Coca-Cola had funded its initial deployment of vending machines through the sale of tokens its machines might one day require. The token holders' interests would have been imperfectly aligned with the interests of investors who owned shares in Coca-Cola, Inc. Rather than caring about share value, they would have cared about token value, which would relate to the supply of the tokens and demand for vended Coke.

For this hypothetical Coca-Cola, it's easy to imagine physical tokens and real vending machines. But for ICOs, the tokens and the "machines"

---

1. See, e.g., Chance Barnett, Trends Show Crowdfunding to Surpass VC After 2016, Medium: Startup Grind (July 22, 2016), https://medium.com/startup-grind/trends-show-crowdfunding-to-surpass-vc-in-2016-65df924d8a82 [https://perma.cc/2BUP-EDFP] ("[H]igh growth entrepreneurs . . . have more sources and channels for finding capital than they've ever had.").

2. See, e.g., Olav Sorenson, Valentina Assenova, Guan-Cheng Li, Jason Boada & Lee Fleming, Expanded Innovation Finance via Crowdfunding, 354 Science 1526, 1526 (2016) (finding that crowdfunding has channeled capital to innovators outside the traditional ambit of venture capital financing).

3. For an introduction to the law, economics, and sociology of peer-to-peer, networked culture, see generally Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom (2006). Finance, too, is entwined with the emerging networked mode of information production. See, e.g., Chris Brummer, Disruptive Technology and Securities Regulation, 84 Fordham L. Rev. 977, 997–1020 (2015); Kathryn Judge, The Future of Direct Finance: The Diverging Paths of Peer-to-Peer Lending and Kickstarter, 50 Wake Forest L. Rev. 603, 613–21 (2015); Elizabeth Pollman, Information Issues on Wall Street 2.0, 161 U. Pa. L. Rev. 179, 202–05 (2012). One goal of this Article is to place questions about the culture and economics of networked information production on the one hand, and finance on the other, within a common frame.

4. Here, as elsewhere, this Article makes general claims in the text but acknowledges exceptions in the footnotes. For instance, ICOs can involve the sale of equity, but it is rare. See infra note 209.

5. While an ICO can occur after a network has been built, the core practice is to raise funds predevelopment. See infra sections II.A–.B.

they operate are digital. They exist on the internet, embodied in software code. The key forms of software are known as "smart contracts"—automated, "if-this-then-that" rules that coders can design to govern the functionality of the digital "crypto" assets sold in ICOs.[6]

Smart contracts may be digital and automated, but they help structure real-world relationships. At present, relationships between ICO promoters and token buyers are quite nebulous.[7] Imagine that those Coca-Cola token investors lacked established legal means to enforce any promises made by Coca-Cola, Inc., cap the supply of tokens, require the use of those tokens to buy Coca-Cola from vending machines, limit sales of Coca-Cola through non-vending-machine channels, or even deploy machines at all. That scenario roughly captures the state of ICO legal contracting and governance today. This is a financial form ripe for fraud, and it has allegedly been used to that precise end.[8]

But fraud also went hand-in-hand with early financial markets;[9] its presence settles little about the fate of the ICO form. According to some, the ICO is an innovative, low-cost method to raise capital and enables a widened range of potential investors to support the development of new, software-based enterprises.[10] In 2017—the year that ICOs entered popular

---

6. Smart contracts were first introduced by Nick Szabo, who drew inspiration from the "humble vending machine." Nick Szabo, Formalizing and Securing Relationships on Public Networks, First Monday (Sept. 1, 1997), https://journals.uic.edu/ojs/index.php/fm/article/view/548/469 [https://perma.cc/KKT6-9PHC].

7. See Initial Coin Offerings (ICOs)—What to Know Now and Time-Tested Tips for Investors, Fin. Indus. Regulatory Auth., http://www.finra.org/investors/alerts/initial-coin-offerings-what-to-know [https://perma.cc/3J2N-MLHN] (last updated Aug. 16, 2018) ("ICO promoters and issuers may be offering the tokens or coins to investors without typical disclosures and customer access to documents required by U.S. regulators like the Securities and Exchange Commission (SEC) that help investors make an informed investment decision.").

8. Shane Shifflett & Coulter Jones, Buyer Beware: Hundreds of Bitcoin Wannabes Show Hallmarks of Fraud, Wall St. J. (May 17, 2018), https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115 (on file with the *Columbia Law Review*) (finding that approximately 20% of ICOs examined by the authors have red flags, including plagiarism in their whitepapers, false promises of returns, and fake founder profiles); cf. John M. Griffin & Amin Shams, Is Bitcoin Really Un-tethered? 4 (June 13, 2018) (unpublished manuscript), https://ssrn.com/abstract_id=3195066 (on file with the *Columbia Law Review*) (arguing that 50% of the rise in Bitcoin price and 64% of rise in other top cryptocurrency prices between March 2017 and March 2018 can be explained as the product of timed market manipulation).

9. See, e.g., Ian Klaus, Forging Capitalism: Rogues, Swindlers, Frauds, and the Rise of Modern Finance 39–47 (2014) (recounting successful trades at the London Stock Exchange in February 1814 based on falsified reports of Napoleon's death).

10. See Nathaniel Popper, Easiest Path to Riches on the Web? An Initial Coin Offering, N.Y. Times: DealBook (June 23, 2017), https://www.nytimes.com/2017/06/23/business/dealbook/coin-digital-currency.html (on file with the *Columbia Law Review*) [hereinafter Popper, Easiest Path]. Nathaniel Popper, an excellent observer of this market at its inception, wrote generally on the bitcoin phenomenon before it reached a wide audience. See Nathaniel Popper, Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money (2015) [hereinafter Popper, Digital Gold].

consciousness[11]—453 ICOs raised an estimated $6.58 billion.[12] By July 1, 2018, an additional 684 ICOs had raised an estimated $17.47 billion.[13] Yet only a few months later, ICO project valuations were at fractions of previous years' highs, causing some analysts to proclaim a "crypto winter."[14]

Twenty-four billion dollars raised over eighteen months is not chump change, but Facebook raised sixteen billion dollars in one day with its 2012 IPO.[15] Though one might not jump to read an entire law review article about Facebook's IPO, an article about the strange world of public coin offerings may present a more compelling proposition. Indeed, an inquiry into ICOs could be fascinating even if (perhaps especially if) the entire ICO market were to dry up tomorrow.

As we aim to show, ICOs have much to teach us about the uneasy relationships between law and technology in our present moment.[16] To students of capital markets, the interest should be obvious. One basic question about our new financial contracting world is simple: How are

---

11. See, e.g., Laura Shin, Here's the Man Who Created ICOs and This Is the New Token He's Backing, Forbes (Sept. 21, 2017), https://www.forbes.com/sites/laurashin/2017/09/21/heres-the-man-who-created-icos-and-this-is-the-new-token-hes-backing/ [https://perma.cc/Z8K8-462P] (identifying 2017 as the year ICOs became a "runaway trend").

12. Cryptocurrency ICO Stats 2017, CoinSchedule, https://www.coinschedule.com/stats.html?year=2017 [https://perma.cc/HGB2-MG4P] (last visited Feb. 2, 2019). This Article will later address the difficulties of calculating accurate network values. See infra note 293. Solely to ease exposition, this Article will generally use market values (in U.S. dollars) reported by widely used coin-data sites.

13. See Cryptocurrency ICO Stats 2018, CoinSchedule, https://www.coinschedule.com/stats.html?year=2018 [https://perma.cc/39GY-6C23] (last visited Feb. 2, 2019) (summing data for months January through June).

14. Charles Bovaird, What Will It Take to Thaw the Crypto Winter?, Forbes (Dec. 13, 2018), https://www.forbes.com/sites/cbovaird/2018/12/13/what-will-it-take-to-thaw-the-crypto-winter/ [https://perma.cc/FVY4-TRT3] ("The market for [ICO]s, in particular, has been hard-hit . . . . Many of the companies that held these token sales in 2017, a time when the entire market was arguably suffering from ICO mania, have been encountering serious challenges."); Samantha Chang, ICO Market Is Dead: Crypto Investor Barry Silbert, CCN (Nov. 28, 2018), https://www.ccn.com/ico-market-is-dead-crypto-investor-barry-silbert/ [https://perma.cc/VS38-5ZT4] (quoting Barry Silbert's assertion that "[t]he ICO market is dead—over" (internal quotation marks omitted))

15. See Evelyn M. Rusli & Peter Eavis, Facebook Raises $16 Billion in I.P.O., N.Y. Times: DealBook (May 17, 2012), https://dealbook.nytimes.com/2012/05/17/facebook-raises-16-billion-in-i-p-o/ [https://perma.cc/V47G-6VJN].

16. We join a nascent literature on this topic. See generally Iris M. Barsan, Legal Challenges of Initial Coin Offerings, 3 Revue Trimestrielle de Droit Financier [RTDF] 54 (2017); Usha R. Rodrigues, Law and the Blockchain, 104 Iowa L. Rev. 679 (2019) [hereinafter Rodrigues, Law and the Blockchain]; Kevin Werbach, Trust but Verify: Why the Blockchain Needs the Law, 33 Berkeley Tech. L.J. 487 (2018) [hereinafter Werbach, Trust but Verify]; Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner & Linus Föhr, The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators (Univ. du Lux. Law Working Paper Series, Paper No. 2017-011, 2018), https://ssrn.com/abstract_id=3072298 (on file with the *Columbia Law Review*) (noting severe disclosure failures in a global and rapidly growing market).

investors protected from exploitation?[17] For regulators, scholars, and investors this issue is an increasingly pressing one. As of early 2019, government agencies at both the federal and state levels have launched ICO investigations, and multiple firms have been charged as fraudulent or criminal enterprises.[18] Even blockchain technologists admit that ICOs

17. Cf. Darian M. Ibrahim, Equity Crowdfunding: A Market for Lemons?, 100 Minn. L. Rev. 561, 587–603 (2015) (describing and dismissing worries that crowdfunding markets might be dominated by low-quality startups with few ways for investors to distinguish better ones from the pack).

18. See In re Coinalpha Advisors LLC, Securities Act Release No. 10582, 2018 WL 6433070, at *2 (Dec. 7, 2018) (charging a digital asset investment fund with violation of Sections 5(a) and 5(c) of the Securities Act); News Release, Colo. Dep't of Regulatory Agencies, Two Companies Promoting Cryptocurrencies Under Scrutiny by Colorado Securities Commissioner 1 (May 3, 2018) (on file with the *Columbia Law Review*) (announcing orders against two ICO teams for potentially violating Colorado securities laws); Press Release, N. Am. Sec. Admin. Ass'n, NASAA Updates Coordinated Crypto Crackdown (Aug. 28, 2018), http://www.nasaa.org/45901/nasaa-updates-coordinated-crypto-crackdown/ [https://perma.cc/4SRN-ENC7] (noting a coordinated enforcement effort by state regulators against ICOs and cryptoassets, resulting in 200 active investigations and 46 enforcement actions); Press Release, N.D. Sec. Dep't, Securities Commissioner Issues Orders Against 3 More Companies Promoting Initial Coin Offerings in North Dakota (Oct 11, 2018), http://www.nd.gov/securities/news/news-archive/securities-commissioner-issues-orders-against-3-more-companies-promoting-initial [https://perma.cc/8Y2W-PV75] (announcing charges against three ICO teams for "promoting unregistered and potentially fraudulent securities in North Dakota"); Press Release, SEC, SEC Charges EtherDelta Founder with Operating an Unregistered Exchange (Nov. 8, 2018), https://www.sec.gov/news/press-release/2018-258 [https://perma.cc/3ZU9-X747] (discussing charges against the operator of a cryptoasset exchange that facilitates ICO token sales); Press Release, SEC, SEC Halts Fraudulent Scheme Involving Unregistered ICO (Apr. 2, 2018), https://www.sec.gov/news/press-release/2018-53 [https://perma.cc/LZ3N-Q2BG] (announcing the charging of "two co-founders of a purported financial services start-up with orchestrating a fraudulent" ICO "that raised more than $32 million from thousands of investors last year"); Press Release, SEC, Two Celebrities Charged with Unlawfully Touting Coin Offerings (Nov. 29, 2018), https://www.sec.gov/news/press-release/2018-268 [https://perma.cc/9MFW-QK8B] (discussing charges against music producer DJ Khaled and boxer Floyd Mayweather Jr. with unlawfully concealing payments they received for promoting ICO tokens); Press Release, SEC, Two ICO Issuers Settle SEC Registration Charges, Agree to Register Tokens as Securities (Nov. 16, 2018), https://www.sec.gov/news/press-release/2018-264 [https://perma.cc/7BN8-QN29] (discussing orders entered against the Airfox and Paragon ICO teams for sales of unregistered securities); Press Release, Tex. State Sec. Bd., $4 Billion Crypto-Promoter Ordered to Halt Fraudulent Sales (Jan. 4, 2018), https://www.ssb.texas.gov/news-publications/4-billion-crypto-promoter-ordered-halt-fraudulent-sales [https://perma.cc/SCN5-F6FC] (noting that the Texas Securities Commissioner entered an "Emergency Cease and Desist Order to halt the multiple investment programs operated by BitConnect, an overseas company that claims a market share of $4.1 billion for its cryptocurrency coins"). For a broader discussion of legal risks accompanying ICOs, see generally Jonathan Rohr & Aaron Wright, Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets 97 (Cardozo Legal Studies Research Paper No. 527, 2018), https://ssrn.com/abstract_id=3048104 (on file with the *Columbia Law Review*) (discussing risk of fraud and abuse).

as a form of fundraising suffer credibility problems, as many projects have still not delivered functional products.[19]

Less obviously, an understanding of the ICO experience can also inform debates about the digital future of capitalism.[20] ICOs represent the increasing financialization of internet-based peer production, and they also reflect the informational ecosystem the internet has wrought. The legal system's interactions with these trends are on display in what follows.

This Article is built around a survey of the 50 ICOs that raised the most capital in 2017 and the role that computer code plays in structuring them. The presence of a cryptoasset at the heart of an offering enables entrepreneurs to deliver investor protections through computer code, rather than through legalistic means. This technological capacity was central to the ideological and practical case advanced by the entrepreneurs who engaged in ICOs. In the 2017 market, founders spoke of automated, "[d]ynamic [c]eiling[s]" for cryptoasset supply;[21] of placing founders' cryptoasset allocations in "time-locked smart contracts" to align incentives for productivity;[22] and of replacing trusted parties with decentralized and verifiable computation.[23] We take an initial look at examples of smart contract design to establish that code does have the potential to become either a substitute for or a complement to old-fashioned legal governance in financial contracting.

But potential is not "reality," and this study shows just how far code falls short of expectations for the top 50 ICOs of 2017. We analyze the relationship between the "paper" promises made by ICO promoters in their offering documents and the actual functionality of the digital assets they deliver. This Article establishes actual functionality by examining the

---

19. See Bovaird, supra note 14 ("Some have criticized the methods used in these token sales, which have frequently involved nothing more than . . . [an] idea outlined in a white paper."); see also Rocco, Futility Tokens: A Utility-Based Post-Mortem, Token Econ. (Oct. 9, 2018), https://tokeneconomy.co/futility-tokens-a-utility-based-post-mortem-d7b1712a5a4e [https://perma.cc/2KW2-4V7K] (dissecting ICO tokens offered by various projects and finding that many could never have supported their touted functionality while generating a profit); Nathaniel Whittlemore, Crypto Narrative Watch: Crypto Winter Edition, Token Econ. (Dec. 19, 2018), https://tokeneconomy.co/crypto-narrative-watch-crypto-winter-edition-bf1cf584def2 [https://perma.cc/CAE2-HH38] (noting that many ICO teams promised their tokens would eventually provide specific functions, but that such functionality was still missing as of late 2018).

20. See, e.g., Julie E. Cohen, The Regulatory State in the Information Age, 17 Theoretical Inquiries L. 369, 375 (2016) ("Emerging, nontraditional regulatory models have tended to be both opaque to external observation and highly prone to capture. New institutional forms that might ensure their legal and political accountability have been slow to develop.").

21. The Status Network: A Strategy Towards Mass Adoption of Ethereum, Status (June 15, 2017), https://status.im/whitepaper.pdf [https://perma.cc/Z233-EPQT].

22. Terms of Token Sale, Storj Labs (BVI) Ltd. 14, https://storj.io/sale-terms.pdf [https://perma.cc/G37K-97S4] (last updated May 18, 2017).

23. See Protocol Labs, Filecoin: A Decentralized Storage Network 8 (2017), https://filecoin.io/filecoin.pdf [https://perma.cc/UL5G-CATU].

smart contracts associated with each ICO, along with the broader software environments through which those smart contracts function. (These are known as "distributed ledgers" or "blockchains," which we discuss further below.) Through careful auditing of the gap between what ICOs promise and what their code delivers, we aim to present coin offerings at a deeper level of institutional detail than is currently present in the literature. Indeed, though legal scholars have begun writing about smart contracts in theory, we are the first to take smart contracts seriously as real-world objects of study.[24]

We evaluate our sample on three aspects of governance that ICO proponents have claimed can be delivered through code and which economic theory suggests should be salient to ICO investors. First, did ICO promoters make any promises (and encode those assurances) to restrict the supply of their cryptoassets? Second, did ICO promoters pledge (and build their promises into smart contracts) to restrict the transfer of any cryptoassets allocated to insiders according to a vesting or lock-up plan? Third, did ICO promoters use code to retain the power to modify the smart contracts governing the tokens they sold, and if so, did they disclose (in natural language) that they had allocated themselves that power? Credible commitments regarding these salient cryptoasset qualities should matter to an investor interested in the economic fundamentals of an ICO.

Our basic finding is that ICO code and ICO disclosures often do not match. In a financial ecosystem built around the proposition that regulation is unnecessary because code is the final guarantee of performance, the absence of coded governance protections is troubling. We also show that at least some popular ICOs have retained the power to modify their tokens' rights but have failed to disclose that ability in plain English.

One takeaway is that no one reads smart contracts,[25] making them a rickety wheel on the ICO investment vehicle. Why might this be, and how significant is it? In evaluating our findings, we consider a few potential explanations for the mismatches between code and disclosure that we observe. We ultimately conclude that while the disjunct is troubling, the normative implications of our project will turn on learning more about who buys ICOs and why.[26]

---

24. See generally Mark C. Suchman, The Contract as Social Artifact, 37 Law & Soc'y Rev. 91 (2003) (articulating a research agenda examining contractual artifacts as such). For two excellent primers on smart contracts, see generally Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code 72–88 (2018); Kevin Werbach & Nicolas Cornell, Contracts *Ex Machina*, 67 Duke L.J. 313 (2017).

25. The obvious allusion is to ordinary contractual fine print. Cf. Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts, 43 J. Legal Stud. 1 (2014) (finding vanishingly low reading rates for end-user license agreements).

26. We hasten to add that the ICO is not inherently a scam: Economic theorists have recently begun developing models that show the potential for cryptoassets to unlock

We proceed as follows. Part I provides clear and precise definitions of various aspects of ICO machinery. It also presents the history of various components: cryptocurrencies, blockchain-based networks, smart contracts, and ICO technology. Part II describes the three ways that we evaluate the quality of an ICO's paper–code match and offers an introduction to the mechanisms by which tokens can vouch for quality. Part III presents the methods of our empirical study. It describes our sources, collections, coding, and smart contract audit procedures. Part IV offers evidence that the ICO market does not vet smart contract code for the qualities we have identified and offers theories as to why. It also suggests how researchers could help regulators and lawmakers in better understanding and overseeing this new business form.

I. AN INTRODUCTION TO TOKENS

To set the stage for our analysis of ICO quality—and our premortem on the current market's pathologies—this Part presents an operational account of ICO components and mechanics.

A. *From Debt and Equity to Native Coin*

Consider a group of entrepreneurs who want to create a soda company. Though they have an amazing recipe, they lack sufficient seed capital to quit their day jobs and market their soda to the world. To access the traditional capital markets, they might form a corporation and seek a business loan, or perhaps a few rounds of private venture capital funding. If successful, they might then choose to issue shares on the New York Stock Exchange (NYSE). In exchange for payment of a price (in dollars) set by investment bankers through careful underwriting, the team would part with shares of its company. The purchasers of those shares would then possess a bundle of rights to govern the corporation, along with residual claims on its assets in proportion to the number of shares they own. Once built, the corporation could charge its customers in dollars, pay its

---

information and value for investors during the early stages of an entrepreneurial venture. See Christian Catalini & Joshua S. Gans, Initial Coin Offerings and the Value of Crypto Tokens 2–5 (MIT Sloan Research Paper No. 5347-18, 2018), https://ssrn.com/abstract=3137213 (on file with the *Columbia Law Review*); Sabrina Howell, Marina Niessner & David Yermack, Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales 1 (NBER Working Paper No. 24774, 2018), http://www.nber.org/papers/w24774 (on file with the *Columbia Law Review*); Thomas Bourveau, Emmanuel T. De George, Atif Ellahie & Daniele Macciocchi, Initial Coin Offerings: Early Evidence on the Role of Disclosure in the Unregulated Crypto Market 5 (July 9, 2018) (unpublished manuscript), https://ssrn.com/abstract=3193392 (on file with the *Columbia Law Review*) (finding a measure of disclosure is correlated with market values). But see Eric Budish, The Economic Limits of Bitcoin and the Blockchain 5–11 (NBER Working Paper No. 24717, 2018), http://www.nber.org/papers/w24717 (on file with the *Columbia Law Review*) (arguing that if bitcoin were an economically important store of value, it would be hacked).

employees and suppliers in the same, and then distribute the leftovers to its shareholders.

The new world of coin-based finance looks different from this traditional model. Instead of issuing contractual claims on the assets of a legal entity (in the form of debt or equity), the team might now issue a token—call it Colacoin—that it promises will be the only way to buy sodas from its (yet to be deployed) vending machines.[27] The team could also pledge that possession of Colacoins would enable their holders to vote on proposed alterations to the vending machine's prices. Further, they could even commit to paying suppliers—bottling companies, truckers, lawyers who work for them—in Colacoin. If, and as long as, the dehydrated people of the world want access to machine-vended cola, then Colacoin will hold value. And if Colacoin is easily exchangeable for dollars, then the nascent company's truckers and lawyers will not mind receiving their initial payments in a strange currency. Replace Coca-Cola with a software-based venture (like a file-sharing service or a platform for streaming video), and Colacoin with a cryptoasset, and you have an ICO.

Obviously, the scenarios differ in a few ways. First, they diverge in terms of how they allocate claims on the entrepreneurs' business. Traditional capital markets require business owners to contractually divest themselves of various rights over their corporation's assets.[28] In contrast, the ICO method can leave economic ownership and legal control unencumbered.[29]

Second, they vary in their source of value. While stock prices should reflect the net present value of the legal rights to the company's expected future cash flows,[30] cryptoasset pricing should reflect an equilibrium between token demand, which is driven by the present value of expected future use and exchange options within the token's native ecosystem, and token supply, which is driven by the token's monetary policy.[31]

---

27. To users, Colacoin thus resembles the coupons, scrips, airmiles, and other cash substitutes that merchants have employed throughout the past century and a half. See Norman I. Silber & Steven Stites, Merchant Authorized Consumer Cash Substitutes 1–2 (Hofstra Legal Studies Research Paper Series, Research Paper No. 2018-03, 2018), https://ssrn.com/abstract=3161453 (on file with the *Columbia Law Review*). Coca-Cola offered a coupon redeemable for one glass of soda as early as 1887. See id. at 2.

28. See, e.g., Ivo Welch, Corporate Finance 4–5 (4th ed. 2017) (discussing tradeoffs between various contractual methods of financing).

29. See Balaji S. Srinivasan, Thoughts on Tokens, Earn.com (May 27, 2017), https://news.earn.com/thoughts-on-tokens-436109aabcbe [https://perma.cc/D7RJ-8DJW]. Clearly, when a token provides rights to purchasers to use a future service, the owner is, in a sense, encumbered. The effect is similar to an airline being encumbered by its loyal customers' airmiles. We mean that tokens do not typically divide the formal rights of ownership into pieces.

30. See, e.g., Aswath Damodaran, Investment Valuation: Tools and Techniques for Determining the Value of Any Asset 11–19 (3d ed. 2012).

31. Work on cryptoasset valuation is in its early stages. See, e.g., Chris Burniske & Jack Tatar, Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond 171–84 (2017) (suggesting cryptoasset valuation models); Catalini & Gans, supra note 26, at 3–5; Aswath

Third, the infrastructure of capital markets enables vetting, trading, and liquidity in established ways. A mighty edifice of regulation and institutional capital stands behind each issuance: Investors know, or at least have the tools to inform themselves about, what they are getting. By contrast, cryptomarkets are new, their players mere years or months old.[32] No Wall Street investment bank has backed an ICO.[33] Indeed, the absence of ICO-specific regulation and intermediaries is seen to be a feature, not a bug, by many enthusiasts.[34]

Finally, and perhaps most significantly to our lawyer-readers, ICOs expand the role played by computer code in governing transactional relationships. Traditional capital-market transactions are heavily mediated

---

Damodaran, The Bitcoin Boom: Asset, Currency, Commodity, or Collectible?, Musings on Mkts. (Oct. 24, 2017), https://aswathdamodaran.blogspot.com/2017/10/the-bitcoin-boom-asset-currency.html [https://perma.cc/GXF2-ZTU3] (suggesting that cryptoassets share characteristics with both currencies and commodities). For recent empirical work on cryptoasset valuation, see generally Hugo Benedetti & Leonard Kostovetsky, Digital Tulips? Returns to Investors in Initial Coin Offerings (May 20, 2018) (unpublished manuscript), https://ssrn.com/abstract=3182169 (on file with the *Columbia Law Review*) (finding that ICO underpricing is driving by Twitter followers and activity); Bourveau et al., supra note 26 (examining the the effects of disclosures on market quality for ICOs); Jongsub Lee, Tao Li & Donghwa Shin, The Wisdom of Crowds and Information Cascades in FinTech: Evidence From Initial Coin Offers (Sept. 1, 2018) (unpublished manuscript), https://ssrn.com/abstract=3195877 (on file with the *Columbia Law Review*) (finding that analyst ratings are associated with increased value); Christian Masiak, Jorn H. Block, Tobias Masiak, Matthias Neuenkirch & Katja Pielen, The Market Cycles of ICOs, Bitcoin, and Ether (July 9, 2018) (unpublished manuscript), https://ssrn.com/abstract=3198694 (on file with the *Columbia Law Review*) (finding that ICO prices interact with the prices of bitcoin and ether); Paul Momtaz, Putting Numbers on the Coins: The Pricing and Performance of Initial Coin Offerings (May 27, 2018) (unpublished manuscript), https://ssrn.com/abstract=3169682 (on file with the *Columbia Law Review*) (finding that ICOs are systematically underpriced, but that long-term performance is mixed); Lauren Rhue, Trust Is All You Need: An Empirical Exploration of Initial Coin Offers (ICOs) and ICO Reputation Scores (May 16, 2018) (unpublished manuscript), https://ssrn.com/abstract=3179723 (on file with the *Columbia Law Review*) (finding that reputation scores from rating sites are not very well correlated with each other or with value, but hype and internet buzz are correlated with value).

32. See, e.g., Darryn Pollock, How Binance Conquered the Cryptocurrency World with Help of a Utility Token, Forbes (Oct. 8, 2018), https://www.forbes.com/sites/darrynpollock/2018/10/08/how-binance-conquered-the-cryptocurrency-world-on-the-back-of-a-utility-token/ [https://perma.cc/FH5P-N29X] (describing the rapid rise of Binance, which was established in 2017).

33. While venture capitalists have taken cryptoassets into their portfolios, see infra section IV.B.4, that is not the same as the underwriting function performed by investment banks in the traditional capital markets. For a model describing when venturers will turn to traditional capital sources instead of ICOs, see generally Jiri Chod & Evgeny Lyandres, A Theory of ICOs: Diversification, Agency, and Information Failure (July 18, 2018) (unpublished manuscript), https://ssrn.com/abstract=3159528 (on file with the *Columbia Law Review*).

34. See Jesse Powell, Kraken's Position on Regulation, Kraken (Apr. 22, 2018), https://blog.kraken.com/post/1561/krakens-position-on-regulation/ [https://perma.cc/X3NC-G9AL] (arguing that regulatory action "doesn't matter to most crypto traders").

by laws, regulations, contracts, and social norms.[35] ICO transactions augment, and perhaps replace, those mediators by embedding controls within the smart contracts through which rules function.[36] At the same time, they also create new roles for lawyers and other legal-adjacent personnel.

The Colacoin clearly would be a far more experimental way to raise capital for the underlying soda company than through the sale of debt or equity.[37] Yet despite their differences, the scenarios share something at a particular level of abstraction: The value of debt, equity, and Colacoin tokens all depend heavily on the success of the entrepreneurial team in building and attracting customers to the product.

B. *Understanding Cryptoassets*

A working conception of ICOs begins with the cryptoassets—the digital coins and tokens—at the center of the operation. Like a physical coin, a cryptoasset is scarce and control over it is transferable. But while physical coins are transmitted hand-to-hand (or hand-to-machine), changes in control of cryptoassets occur through the networks that host them (via the transfer of a digital key).[38] Indeed, a cryptoasset is nothing more than an entry in a ledger that specifies that a particular user, identified by a certain "private key" (essentially, a fancy password) is the sole party able to exercise a discrete set of powers associated with the ledger entry. While their private keys might travel hand-to-hand in the physical world, the actual cryptoasset is destined to remain a mere ledger entry, forever locked inside its "native" protocol.[39]

---

35. Though market fundamentalists might occasionally forget this, it is essential to any understanding of the contemporary economy. See, e.g., David Singh Grewal, Laws of Capitalism, 128 Harv. L. Rev. 626, 652 (2014) (reviewing Thomas Piketty, Capital in the Twenty-First Century (2014)) ("Capitalism is fundamentally a legal ordering: the bargains at the heart of capitalism are products of law."); Katherina Pistor, A Legal Theory of Finance, 41 J. Comp. Econ. 315, 315 (2013) ("[L]aw and finance are locked into a dynamic process in which the rules that establish the game are continuously challenged by new contractual devices, which in turn seek legal vindication.").

36. This places them in the tradition of code-based controls studied most closely in the context of intellectual property. See, e.g., Julie E. Cohen, Pervasively Distributed Copyright Enforcement, 95 Geo. L.J. 1, 2 (2006) (discussing this in the context of copyright enforcement).

37. Cryptoasset sales can be viewed as a new strategy for "decoupling" economic ownership from the control of business ventures that Henry Hu has documented. See Henry T.C. Hu, Financial Innovation and Governance Mechanisms: The Evolution of Decoupling and Transparency, 70 Bus. Law. 347, 351, 354–63 (2015).

38. See Rainer Böhme, Nicolas Christin, Benjamin Edelman & Tyler Moore, Bitcoin: Economics, Technology, and Governance, 29 J. Econ. Persp. 213, 213 (2015). Network communication protocols are the linguistic conventions that enable transmissions of intelligible information between participants in a network. See generally Andrew S. Tannenbaum & David J. Wetherall, Computer Networks 29–40, 75–81 (5th ed. 2011).

39. By this we mean that the cryptoasset is never itself transferred. While the record denoting its ownership may be modified, the asset is doomed to remain but an abstraction represented within the ledger on which it originated.

Cryptoasset history begins with Bitcoin currency and the Bitcoin ledger (also known as a "blockchain").[40] Prior to their advent, money was either held in physical form (for example, coins or paper notes) or on the ledger of a centralized intermediary (for example, bank deposits or PayPal balances).[41] Bitcoin is the first significant digital currency system that needs no centralized intermediary to maintain proper books.[42] The key to the ledger's design—and that of the public blockchain-based systems in its wake—is how it maintains a trustworthy record of ownership rights. Rather than being centralized within a single firm, the Bitcoin ledger is *replicated and distributed* across a network of computers that communicate with each other via the internet.[43] These computers are called "nodes."[44] When a holder of bitcoins distributes a message to the network's nodes asking to transmit some bitcoins to another user, the transactors need not rely on the trustworthiness of any actor in the system to revise their copy of the ledger appropriately.[45] Rather, they rely on economic incentives and code-based controls that govern the nodes' behavior to ensure that all copies of the ledger are updated identically.[46]

The shift toward a broad range of blockchain-based business plans was realized in another network: Ethereum. The designers of Ethereum produced a general-purpose computational system that operates through a public blockchain.[47] To perform computations on this decentralized "world computer," users must pay a per-function fee of "ether"—a "gas" charge—which functions as Ethereum's currency.[48] As a result, the value of ether depends significantly on the supply of, and demand for,

---

40. On the prehistory and history of Bitcoin, see generally Arvind Narayanan & Jeremy Clark, Bitcoin's Academic Pedigree, ACM Queue (Aug. 29, 2017), https://queue.acm.org/detail.cfm?ref=rss&id=3136559 [https://perma.cc/ZA6A-BJL9]; Popper, Digital Gold, supra note 10.

41. See Morgan Ricks, The Money Problem: Rethinking Financial Regulation 58 (2016) (distinguishing between certificated and uncertificated forms of money).

42. See generally De Filippi & Wright, supra note 24, at 61–71; Kevin Werbach, Blockchain and the New Architecture of Trust (2018).

43. See Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder, Bitcoin and Cryptocurrency Technologies 27–50 (2016); Böhme et al., supra note 38, at 216.

44. Narayanan et al., supra note 43, at 7–10.

45. See Werbach, Trust but Verify, supra note 16, at 512–13.

46. See id. This reliance on incentives and code-based controls, rather than social control mechanisms like law and norms, was a central objective of early cryptocurrency visionaries. See Popper, Digital Gold, supra note 10, at 119–20. But it does not mean that Bitcoin is necessarily impossible to hack. See Ittay Eyal & Emin Gün Sirer, Majority Is Not Enough: Bitcoin Mining Is Vulnerable, Comm. ACM, July 2018, at 95, 95.

47. See Werbach & Cornell, supra note 24, at 333–35; Rohr & Wright, supra note 18, at 19.

48. Ethereum Whitepaper: A Next Generation Smart Contract and Decentralized Application Platform, Github, https://github.com/ethereum/wiki/wiki/White-Paper [https://perma.cc/46KY-4V3W] (last visited Feb. 4, 2019). The "gas" charged is proportional to the complexity of the computation requested. Id.

computational power active on the Ethereum system. One of the key reasons for Ethereum's popularity is its support for snippets of computer code that interact with the ledger known as smart contracts.[49] One can think of smart contracts as a prewritten set of system-performance rules. Just as legal contracts govern the allocation of paper money among transactors, smart contract code governs the transmission of ether, or other stored assets, among transactors on the Ethereum system.[50]

To understand how Ethereum works, imagine that you drop a quarter into a vending machine slot and down falls a can of Coca-Cola. This "humble" mechanism serves as the inspiration for wide-ranging creativity on Ethereum, where smart contract engineers write scripts about how the system will behave in response to various inputs.[51] These inputs might include basic information about where to send ether, and also more complex information, like data from a weather vane.[52] Ether plays the role of both the vending machine's quarters and its most important payload—the Coca-Cola of the system. Indeed, because ether acts as a decent (if volatile) currency, one can engage in smart contracting that attempts to mimic paper-age agreements for insurance,[53] escrow,[54] or even something akin to corporate formation.[55]

To build increasingly complex and interoperating mechanisms within Ethereum, its community has begun developing standards—"fill

---

49. See generally Karen E.C. Levy, Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law, 3 Engaging Sci. Tech. & Soc'y 1 (2017); Werbach & Cornell, supra note 24; Jeremy M. Sklaroff, Comment, Smart Contracts and the Cost of Inflexibility, 166 U. Pa. L. Rev. 263 (2017).

50. In most ways, calling these code snippets "contracts" is quite misleading, but we are stuck with the dominant terminology. For careful discussions, see generally J.G. Allen, Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Language, 14 Euro. Rev. Cont. L. 307 (2018); James Grimmelmann, All Smart Contracts Are Ambiguous, J.L. & Innovation (forthcoming 2019) (on file with the *Columbia Law Review*).

51. It also served as inspiration for Szabo's initial coinage of the smart contract idea. See supra note 6 and accompanying text.

52. That is, some device might transmit readable data to an Ethereum-based smart contract from the outside world—for instance, a website—via an "oracle." See Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels & Elaine Shi, Town Crier: An Authenticated Data Feed for Smart Contracts, 2016 Proc. 2016 SIGSAC Conf. on Computer & Comm. Security 270, 270; Houman Shadab, What Smart Contracts Need to Learn, Lawbitrage (Sept. 4, 2014), http://lawbitrage.typepad.com/blog/2014/09/smartcontracts.html [https://perma.cc/H8AD-QAG9].

53. See, e.g., AXA Beta, About Us, Fizzy, https://fizzy.axa/en-gb/faq [https://perma.cc/EG6J-EHQT] (last visited Jan. 26, 2019) (describing an Ethereum-based flight insurance system).

54. See, e.g., LocalEthereum, How Our Escrow Smart Contract Works, LocalEthereum's Blog (Oct. 26, 2017), https://blog.localethereum.com/how-our-escrow-smart-contract-works/ [https://perma.cc/QSM3-Y56C].

55. Attempt is a key word here: The leading example of a quasi-corporate form on the Ethereum blockchain was a smart contract known as "the DAO," which failed spectacularly. See Rodrigues, Law and the Blockchain, supra note 16, at 697–708 ("The 2016 DAO is a cautionary tale about the limits of relying on a 'code is law' model when (as inevitably happens) gaps in the nexus of contracts emerge without a legal intervention point on which the law can work.").

in the blank" templates that perform agreed-upon functions. One of those—standard "ERC-20"[56]—plays a large role in our story. It establishes a simple template to create (or "mint," in crypto-lingo) and operate entirely new cryptoassets within the Ethereum system. This is what the description of the standard looks like in code:

FIGURE 1: THE ERC-20 INTERFACE[57]

```
contract ERC20Interface {

     function totalSupply() public view returns (uint);

     function balanceOf(address tokenOwner) public view
         returns (uint balance);

     function allowance(address tokenOwner, address
         spender) public view returns (uint remaining);

     function transfer(address to, uint tokens) public
         returns (bool success);

     function approve(address spender, uint tokens) public
         returns (bool success);

     function transferFrom(address from, address to, uint
         tokens) public returns (bool success);

     event Transfer(address indexed from, address indexed
         to, uint tokens);
     event Approval(address indexed tokenOwner, address
         indexed spender, uint tokens);
}
```

Creating a new cryptoasset typically requires a minimum of approximately fifty lines of code and three decision components: the asset's name, its ticker symbol, and the number of units—or "tokens"—to mint.

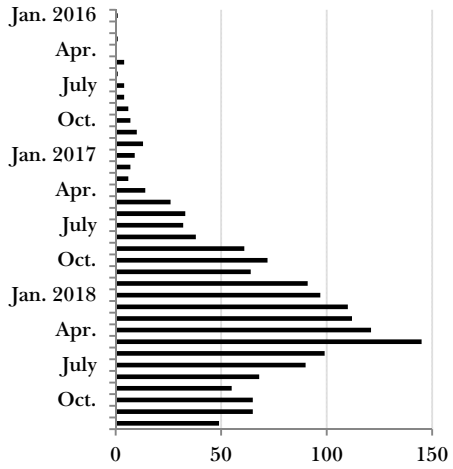
56. See Fabian Vogelsteller & Vitalik Buterin, ERC-20 Token Standard, GitHub, https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md [https://perma.cc/4GZA-EFMP] (last visited Jan. 26, 2019). The acronym "ERC" means "Ethereum Request for Comment." Chris Dannen, Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners 106 (2017). The "Request for Comment" is a form of memorandum used to draft networking protocols and standards, most prominently used by the Internet Engineering Task Force in designing core internet technologies. See RFC Editor, Informational RFC 5540: 40 Years of RFCs, Internet Eng'g Task Force (Apr. 7, 2009), https://tools.ietf.org/html/rfc5540 [https://perma.cc/RS4N-TU8F]. The Ethereum community has adopted this form of consensus-based standard to develop common design patterns for smart contracts. See Dannen, supra, at 111.

57. ERC20 Token Standard, Ethereum Wiki, https://theethereum.wiki/w/index.php/ERC20_Token_Standard [https://perma.cc/8AXZ-LE4X] (last updated Dec. 4, 2018). A cryptoasset that meets the ERC-20 standard contains a block of code for each of the named functions and events above. See supra note 56 and accompanying text.

C. *ICOs Hit the Bigtime*

In 2014, Ethereum raised real money by selling ether to the public.[58] The next major ICO was Augur, which concluded in October 2015.[59] The market grew slowly until 2017, when it hit the gas.

FIGURE 2: NUMBER OF ICOS BY MONTH[60]

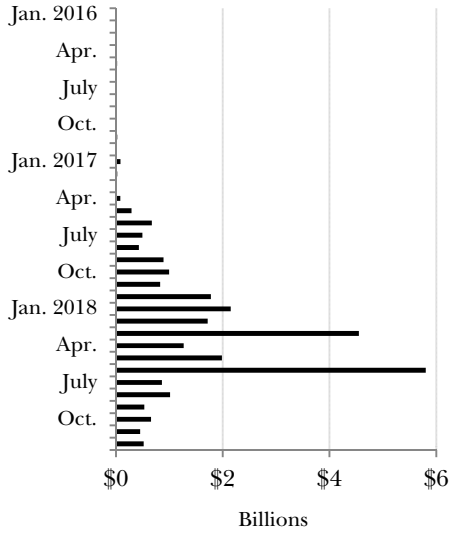


58. Ethereum sold tokens directly to the unaccredited public but did not initially enable a secondary market. See Vitalik Buterin, Launching the Ether Sale, Ethereum Blog (July 22, 2014), https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/ [https://perma.cc/PK7W-XBMD] (stating, in the announcement of Ethereum's ICO, that ether would be purchasable directly from the Ethereum website but would not immediately be usable or transferable). Some subsequent token sales have been private (sometimes called "presales"), see, e.g., Chloe Cornish & Richard Waters, Silicon Valley Investors Line Up to Back Telegram ICO, Fin. Times (Jan. 25, 2018), https://www.ft.com/content/790d9506-0175-11e8-9650-9c0ad2d7c5b5 (on file with the *Columbia Law Review*), but the archetypal version is public—democratized, in the tradition of Kickstarter and other "peer-to-peer" financial platforms. See supra notes 3, 17 and accompanying text.

59. See Augur: Welcome to the Future of Forecasting, ICObench, https://icobench.com/ico/augur [https://perma.cc/43KA-CNUW] (last visited Jan. 26, 2019). Between the Ethereum ICO, which concluded in September 2014, and the Augur ICO, which concluded in October 2015, there were several small ICOs that raised under $2 million. See, e.g., ICOs and Crowdsales: Over $270 Million Raised and Counting, Smith & Crown (Dec. 1, 2016), https://www.smithandcrown.com/icos-crowdsale-history/ [https://perma.cc/M66D-3H2T].

60. This chart was prepared to illustrate general monthly trends in the number of ICOs launched during the period between January 1, 2016, and December 31, 2018. The data underlying this chart—which excludes the DAO ICO in 2016—were collected from coinschedule.com as of December 31, 2018. Since December 31, 2018, coinschedule.com has made some minor classification and presentation changes to this data. These classification and presentation changes have resulted in deviations of less than 1% (on a total basis) from the data presented graphically herein. This holds for both the number of ICOs in the last three years (Figure 2) and the total amounts raised by ICOs in the last three years (Figure 3). For the most current data available from coinschedule.com, see Crypto Token Sales Market Statistics, CoinSchedule, www.coinschedule.com/stats.html [https://perma.cc/W9T3-AZW9] (last visited Feb. 16, 2019).

FIGURE 3: TOTAL RAISED IN THE ICO MARKET BY MONTH[61]



As the ICO market exploded so too did regulatory interest in its activities.[62] Such scrutiny is no surprise: ICOs, like many internet-based phenomena before them, intentionally take place at the regulatory perimeter.[63] They exploit a basic tension between the cross-jurisdictional and pseudonymous aspects of cryptocurrency transactions on the one hand and the objectives of regulators on the other.[64] The question of just

61. This chart was prepared to illustrate general monthly trends in the total funds raised by ICOs launched during the period between January 1, 2016, and December 31, 2018. For further discussion of how this data set was obtained, see supra note 60. The spike in March 2018 represents when the EOS raise was realized in the dataset, though it occurred continuously before then.

62. See Alex Sunnarborg, The Incoming Wave of ICO Regulation (Yes, It's Coming), Coindesk (Nov. 2, 2018), https://www.coindesk.com/the-incoming-wave-of-ico-regulation-yes-its-coming [https://perma.cc/U3GZ-DFVW].

63. See Elizabeth Pollman & Jordan M. Barry, Regulatory Entrepreneurship, 90 S. Cal. L. Rev. 383, 392–97 (2017) (defining "regulatory entrepreneurship" as a business activity in which legal uncertainty regarding a core aspect of the business necessitates that the business attempt to change or shape the law, and noting that "[r]egulatory entrepreneurship often happens when businesses are built upon new technology"); Tim Wu, Strategic Law Avoidance Using the Internet: A Short History, 90 S. Cal. L. Rev. Postscript 7, 7 (2017), https://southerncalifornialawreview.com/2017/03/01/strategic-law-avoidance-using-the-internet-a-short-history-postscript-response-by-tim-wu/ [https://perma.cc/P6JS-KTK7] (stating that tech-sector entrepreneurs, starting in the late 1990s and continuing to the present, have recognized "that the Internet might provide profitable opportunities at the edges of the legal system").

64. See, e.g., Sean Foley, Jonathan R. Karlsen & Tālis J. Putniņš, Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?, 33 Rev. Fin. Stud. (forthcoming 2019) (on file with the *Columbia Law Review*) (finding that approximately one half of bitcoin transactions are associated with illicit activity).

how significant the demand is for cryptoassets among money launderers and tax evaders is not one we answer here, but it sits as a backdrop to the inquiry that follows.

In the traditional IPO context, the Securities and Exchange Commission (SEC) and state securities regulators oversee issuer activity from soup to nuts.[65] They mandate registration of securities issuances, require pages and pages of disclosures over the life cycle of a security, restrict the trading activities of various parties, and possess myriad investigation and enforcement powers to effectuate their portfolio of laws and regulations.[66] As of 2018, no similarly clear regime was in place for ICOs.[67] In lieu of the heavily lawyered products of IPO documentation, the ICO market agreed upon a less formal document known as a "whitepaper."[68]

Like governmental and nonprofit whitepapers that seek to exemplify authoritative subject mastery while gesturing toward collaborative openness, cryptoasset whitepapers are public documents that describe promoters' plans for development and solicit community involvement.[69] Authoritative copies are typically available in PDF form on promoters' websites and are provided through listing services like coinschedule.com.[70] This makes whitepapers a transparent form of investor information but obviates the need for outside vetting before they go live.

Unsurprisingly, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is using its authority to combat money laundering and criminal activity involving cryptoassets. See Letter from Drew Maloney, Assistant Sec'y for Legislative Affairs, U.S. Dep't of the Treasury, to the Honorable Ron Wyden, Ranking Member, U.S. Senate Comm. on Fin. 1 (Feb. 13, 2018), https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf [https://perma.cc/2P6B-K8VD] (stating that "[c]ombating the abuse of existing and emerging payment systems by illicit financiers"—including various cryptoasset-based systems—"is a priority issue for FinCEN").

65. See What We Do, SEC, https://www.sec.gov/Article/whatwedo.html [https://perma.cc/75DL-EUXT] (last visited Jan. 27, 2019).

66. See id.

67. However, SEC Chairman Jay Clayton has suggested that "tokens and offerings that feature and market the potential for profits based on the entrepreneurial or managerial efforts of others contain the hallmarks of a security under U.S. law." Initial Coin Offerings (ICOs), SEC, https://www.sec.gov/ICO [https://perma.cc/835G-LQ8K] (last updated Feb. 22, 2019); see also Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207, 2017 WL 7184670, at *1 (July 25, 2017) [hereinafter Report of the DAO] ("[T]he Commission has determined that DAO Tokens are securities under the Securities Act of 1933 ('Securities Act') and the Securities Exchange Act of 1934 ('Exchange Act').").

68. See Barsan, supra note 16, at 54 ("Every ICO starts with a whitepaper, very similar to a prospectus, that describes the project and the rights given to investors.").

69. Appendix C contains several examples of language obtained from these whitepapers. See Shaanan Cohney, David Hoffman, Jeremy Sklaroff & David Wishnick, Coin-Operated Capitalism—Appendix C: Individual ICO Claims (Apr. 2019), https://columbialawreview.org/content/coin-operated-capitalism-appendix-c/ (on file with the *Columbia Law Review*) [hereinafter Appendix C].

70. See id.

The legal status of whitepapers (and accompanying tweets, Medium posts, Reddit comments, and social media buzz) is unclear at best. Sometimes, whitepapers refer to—and embed—contractual terms and conditions of sale.[71] In such cases, they provide information about product attributes, which would function as contractual warranties. In other cases, they resolutely speak in future tenses, offering difficult-to-parse details about what is promised and what is merely aspirational.[72] Absent clearly communicated and defined offers, it is unlikely that buying a token in reliance on such documents constitutes a traditional contract, though other regimes of consumer protection law (state consumer Unlawful Trade Practices statutes, false advertising, securities laws) might fill the regulatory gap.

Beyond the informational environment, ICO issuances also differ from IPO issuances in terms of where they are traded. While public equities trade on established secondary markets like the NYSE or NASDAQ, cryptoassets trade on hundreds of upstart markets, sometimes under light-to-nonexistent regulation.[73] They are located in diverse jurisdictions and have been embroiled in a range of legal controversies.[74]

Despite these significant divergences between IPOs and ICOs, the near-identical nomenclature is no mistake. Both entail the issuance of assets whose value depends on the success of a business venture, and both are offered to so-called "retail" investors. These essential similarities in economic function have not been lost on federal securities regulators in the United States, who lately have begun to apply the wonderfully medium-agnostic securities laws to regulate ICOs.[75] A number of state

---

71. See id.

72. See id.

73. See Steven Russolillo & Eun-Young Jeong, Cryptocurrency Exchanges Are Getting Hacked Because It's Easy, Wall St. J. (July 18, 2018), https://www.wsj.com/articles/why-cryptocurrency-exchange-hacks-keep-happening-1531656000 (on file with the *Columbia Law Review*) (noting that "[r]egulatory gaps" create conditions for widespread hacking); Kai Sedgwick, The Number of Cryptocurrency Exchanges Has Exploded, Bitcoin.com (Apr. 11, 2018), https://news.bitcoin.com/the-number-of-cryptocurrency-exchanges-has-exploded/ [https://perma.cc/28LB-TYM2] (documenting over 500 exchanges).

74. See, e.g., Matthew Leising, U.S. Regulators Subpoena Crypto Exchange Bitfinex, Tether, Bloomberg (Jan. 30, 2018), https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc (on file with the *Columbia Law Review*); Kosaku Narioka, Court Blocks Payday for Chief of Bankrupt Mt. Gox Bitcoin Exchange, Wall St. J. (June 25, 2018), https://www.wsj.com/articles/court-blocks-payday-for-chief-of-bankrupt-mt-gox-bitcoin-exchange-1529929409 (on file with the *Columbia Law Review*).

75. At first, the SEC moved gingerly in response to the novelty of the ICO form, leaving open the question of whether cryptoassets fell into a bona fide statutory and regulatory gap. Cf. Eric Biber, Sarah E. Light, J.B. Ruhl & James Saltzman, Regulating Business Innovation as Policy Disruption: From the Model T to Airbnb, 70 Vand. L. Rev. 1561, 1583–84 (2017) (describing the business strategy of exploiting gaps in existing law as "policy disruption"). In 2017, the SEC took a number of public actions concerning ICOs that began answering the question. See, e.g., In re Munchee Inc., Securities Act Release

regulators are also actively policing bad actors in the ICO market.[76]

Assuming the ICO market matures, these outlier-policing activities will likely be augmented with broader regulatory schemes aimed at standardizing disclosures for the mine run of ICOs.[77] For that effort to be successful, it is imperative for policymakers to understand the contours of ICO transactions, and the institutional environment in which they take place, in detail. We turn to offering such detail now.

II. SMART CONTRACTS IN THE WILD

This Part seeks to better understand some of the basic economics of cryptoassets, and the roles that code—specifically, smart contracts—might be playing. The central relationship we investigate is that between "paper" and "code."[78] Ever since the cryptographer (and law graduate) Nick Szabo first introduced the concept of smart contracts, their artisans have sought to use code to replace and augment traditional institutions for ensuring performance within transactional relationships. The utopian ideal is a "grand merger of law and computer security,"[79] which might render the protections offered by the former to be at best superfluous.[80]

That hope is emphatically present in some of the offering and promotional materials that crypto investors receive. These materials speak of sales where smart contracts will "stop accepting commitments at

---

No. 10445 (Dec. 11, 2017), https://www.sec.gov/litigation/admin/2017/33-10445.pdf [https://perma.cc/63QB-6CRB]; Report of the DAO, supra note 67; Complaint at 5–7, SEC v. Plexcorps, No. 17-CV-7007 (E.D.N.Y. Dec. 14, 2017), 2017 U.S. Dist. LEXIS 206145. Prominently, in early 2018, Commissioner Clayton used his bully pulpit to state that "many promoters of ICOs and cryptocurrencies are not complying with our securities laws." See Jean Eaglesham & Paul Vigna, Cryptocurrency Firms Targeted in SEC Probe, Wall St. J. (Feb. 28, 2018), https://www.wsj.com/articles/sec-launches-cryptocurrency-probe-1519856266 (on file with the *Columbia Law Review*).

76. See State and Provincial Securities Regulators Conduct Coordinated International Crypto Crackdown, N. Am. Sec. Admin. Ass'n (May 21, 2018), http://www.nasaa.org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/ [https://perma.cc/XC7D-WSPY].

77. See, e.g., Shlomit Azgar-Tromoer, Crypto Securities: On the Risks of Investments in Blockchain-Based Assets and the Dilemmas of Securities Regulation, 68 Am. U. L. Rev. 69, 104–11 (2018) ("[I]nformational asymmetries in the blockchain territory may warrant securities regulation."); Rohr & Wright, supra note 18, at 97 (calling upon the SEC to establish a regulatory framework that addresses fraud prevention, investor protection, and capital formation).

78. For the purposes of this Article, "paper" refers to the prose-bound texts of traditional agreements, offering materials, and promotional copy that accompany ICOs. These documents live mainly on the internet, but resemble their physical-paper predecessors in form. Conversely, "code" refers to the blockchains and associated smart contracts that govern the cryptoassets sold through ICOs.

79. Szabo, supra note 6.

80. Id.

888,888ETH hard cap,"[81] of automated destruction of excess cryptoasset supply,[82] and of "Reserve Tokens . . . locked in a smart contract" according to predetermined specifications.[83] They promise with precision that "new founders' tokens [are] distributed pursuant to the launch of an EOSIO Platform in a smart contract and [that the default EOSIO Software configuration] releases 100,000,000 of such tokens . . . linearly to Block.one every second over a period of 10 years."[84] While markets of unsophisticated investors typically require investor protection laws and intermediaries to protect against market manipulation,[85] the "crypto industry" has "greater transparency, fewer middle men . . . [and] programmatically enforceable contracts."[86] That is, this community tries to make concrete the ideological project of using code to replace the rules of entity governance that law currently creates.

Practical realities also motivate a turn to code in this space. Even if the paper surrounding ICOs created legally binding obligations—which it sometimes will not[87]—legal rights are only as valuable as their practical enforceability.[88] Because cryptoassets can move freely and pseudonymously through the internet, it can be difficult to pin them down to particular jurisdictions.[89] And the promoters of many ICOs have set up shop in ways that make it challenging for U.S. courts and regulators to reach their assets.[90] Thus, promises that are made in marketing documents and

---

81. Monaco, Whitepaper, Crypto Rating 8, https://cryptorating.eu/whitepapers/Monaco/monaco-whitepaper.pdf [https://perma.cc/YSB2-GF36] (last visited Feb. 4, 2019).

82. Monetha, Whitepaper 35–36 (2017), https://ico.monetha.io/Monetha_WP.pdf [https://perma.cc/WE6M-859F].

83. Monaco, supra note 81, at 11.

84. Frequently Asked Questions, EOS, https://eos.io/faq (on file with the *Columbia Law Review*) (last visited Feb. 4, 2019).

85. See, e.g., 1 Louis Loss, Joel Seligman & Troy Paredes, Fundamentals of Securities Regulation 4 (7th ed. 2018).

86. Powell, supra note 34.

87. See supra text accompanying notes 34–36, 64–77.

88. But see Cass R. Sunstein, On the Expressive Function of Law, 144 U. Pa. L. Rev. 2021, 2032 (1996) (discussing cases "when the relevant law announces or signals a change in social norms unaccompanied by much in the way of enforcement activity"); Tess Wilkinson-Ryan & David A. Hoffman, The Common Sense of Contract Formation, 67 Stan. L. Rev. 1269, 1300 (2015) ("In these studies, we found not only that subjects' intuitions about contract formation diverge from the legal rules, but that commitment to promissory obligations is more deeply entrenched than mere legal enforceability.").

89. See, e.g., Receiver's Initial Status Report for Receivership Estate of Arisebank at 3–7, SEC v. Arisebank, No. 3:18-cv-0186-M (N.D. Tex. Feb. 26, 2018), ECF No. 53 (detailing a receiver's difficulties in recovering cryptoassets).

90. See id.; see also SEC Office of Investor Educ. & Advocacy, SEC Pub. No. 153, Investor Alert: Ponzi Schemes and Virtual Currency (2013), https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf [https://perma.cc/AKC6-R59V]; David Z. Morris, The Rise of Cryptocurrency Ponzi Schemes, Atlantic (May 31, 2017), https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/ [https://perma.cc/FJU7-NSYW].

terms and conditions of sale, even if legally binding, might lack an easy and practical form of legal remedy.

Given this background, an ICO that promises particular, encodable governance terms but does not encode them is not delivering on an archetypal feature of this financial form. According to those who argue the form is novel—so novel as to deny the need for wise intermediaries, venture capitalist (VC) vetters, and regulators with teeth—it is the immutable, transparent code that enables (and creates) a trustless but trusted market.[91] With that foundational, code-centered principle in mind, we ask the classic question that motivates so much of the law of finance and corporate governance: How can investors turn over productive control of their money to entrepreneurs while also protecting themselves against exploitation?

This is a timeworn problem. In the old-growth public markets, investors can rely on disclosure regimes (imperfectly backed by public agency enforcement) and fiduciary rules (imperfectly backed by court enforcement) to manage risk. In private firms—ranging from family-owned businesses to VC-backed startups—contracts must generally suffice. What is new here (if anything) is that the cryptoasset community proposes a technological solution—the token's coded rules—to manage some crucial sources of agency cost.[92]

One type of bargained-for protection is a constraint on the *supply* of the investment asset for sale. In the traditional corporate context, each share sold to investors provides a legal right to a piece of an enterprise's residual assets. In an efficient market, changes to the number of outstanding shares would affect share price but not firm value.[93] Put another way, the enterprise's assets are like a pie, and every newly issued share makes each slice smaller. Because they want big pieces, early shareholders seek protection against late-breaking stock issuance.[94] Traditional corporations act through human agents; those humans are only able to issue as many shares as the corporation's (amendable) Articles

---

91. See Kemane Ba, Konduktum - SMT Proposal /Tackling Copyrights/ Voting for "Proof of Authorship," Steemit (Jan. 28, 2018), https://steemit.com/utopian-io/@kemane/konduktum-smt-proposal-tackling-copyrights-voting-for-proof-of-authorship [https://perma.cc/P7DD-H6G9]; cf. Timothy C. May, The Crypto Anarchist Manifesto, Activism.net, https://www.activism.net/cypherpunk/crypto-anarchy.html [https://perma.cc/2WQA-LSM8] (last visited Feb. 16, 2019) (arguing that "cryptographic protocols" will provide "nearly perfect assurance against tampering" in the new world of crypto anarchy).

92. For an agency-costs model of the choice between VC and ICO forms, see Chod and Lyandres, supra note 33, at 14–24.

93. See, e.g., Paul Asquith & David W. Mullins, Jr., Equity Issues and Offering Dilution, 15 J. Fin. Econ. 61, 62 (1986) ("Thus with close substitutes, efficient capital markets and fixed investment policies, the price of any firm's shares should be independent of the number of shares the firm, or any shareholder, chooses to sell.").

94. See, e.g., Steven N. Kaplan & Per Strömberg, Financial Contracting Theory Meets the Real World: An Empirical Analysis of Venture Capital Contracts, 70 Rev. Econ. Stud. 281, 291–92 (2003).

of Incorporation allow.[95] Exploitative issuances are deterred by the common law of fiduciary duty.[96]

Supply constraints matter to cryptoasset investors, as well. Remember, tokens are not typically claims on the enterprise's residual assets.[97] Rather, they normally provide investors the right to use or govern the actual system whose hypothesized construction is funded by their money.[98] Shareholders in Coca-Cola care about the value of their residual claims on Coca-Cola, Inc.'s assets. But the holders of Colacoin care about the demand for, and supply of, use-rights to the future system. The number of use-rights available—in other words, the "money supply" of circulating tokens—is thus a central determinant of individual token price.[99] The value of a token, like the value of a stock, can be diluted through new issuance. Just as our Colacoin owners hope that legions of thirsty people demand vending-machine cola, they also pray that Coca-Cola will not engage in rampant inflation of the token supply. Similarly if Coca-Cola promises to remove tokens from circulation (so-called 'burning'), Colacoin owners would expect the value of their investment to rise.

ICOs, unlike corporations, are not birthed through the filing of Articles of Incorporation that limit stock issuance. There is no analog to the fiduciary rules, or the Delaware Chancery Court, that govern when dilution can occur. Cryptoassets are instead created, limited, and used up according to code controlling the contents of a blockchain.[100] Thus, a purchaser's protection against wanton inflation of supply comes directly from the cryptoasset code.[101] That is not to say that ICO promoters might not also make soft-law promises about supply—in fact, they often do, and such promises likely bear on value.[102] But when such promises are not manifest in the code, investors' ability to enforce constraints will be limited to their very uncertain ability to sue and recover founders' assets. Because ICO project founders can do business entirely over the internet, they may be hard to find and sue. Further, it remains to be seen which causes of action might be successfully pursued in the ICO context.[103]

---

95. See, e.g., Del. Code tit. 8, § 157 (2019).

96. See, e.g., In re Tri-Star Pictures, Inc., 634 A.2d 319, 328 (Del. 1993).

97. See supra note 27 and accompanying text.

98. See supra text accompanying notes 28–29.

99. The supply of tokens might affect a project in other ways, as well. A project with too few circulating tokens might unnecessarily limit scalability, thereby depressing project value. This makes the price function for tokens multimodal, a dynamic not present in pricing shares of stock.

100. See generally De Filippi & Wright, supra note 24.

101. As one group of commentators notes, the Bitcoin blockchain "can be understood as the first widely adopted mechanism to provide absolute scarcity of a money supply." Böhme et al., supra note 38, at 215.

102. Bourveau et al., supra note 26, at 19 (using whitepaper promises of soft cap to predict an increase in price).

103. See infra note 185 and accompanying text.

A second bargained-for protection has to do with the threat that key members of the entrepreneurial team will walk away from the project. Investors generally protect against desertion (and motivate exertion) through a set of carrots and sticks offered to managers. They incentivize them with equity options—rights that enable managers to share in the firms' future profits—but condition those options' exercise on contractual conditions, in other words, vesting.[104] Option, lock-up, and vesting rules attempt to align managers' incentives with those of the firm and are endemic in the early-stage VC financing world.[105]

In ICOs, classic options are quite rare, but token-vesting promises are common.[106] As one project (marketing its vesting promises) wrote, it "is a governance practice designed to ensure long-term alignment of interests and is standard for any serious project."[107] Another wrote that "[v]esting is a must. There are no excuses not to do it. It aligns everyone's incentives and ensures that no founder dumps happen."[108]

As with promises regarding supply, vesting promises that are coded are enforced automatically.[109] Those merely present in marketing materials or paper contracts are less likely to be enforceable.[110] Uncoded vesting promises might (or might not) be present in governing documents of the underlying formal organizations. They likely would be located in the

---

104. We appreciate that token vesting is different from the traditional equity mode and that a more precise term might be "lock-up." We follow the nascent industry terminology for clarity. See, e.g., Dana Edwards, Criteria for Determining Fair Distribution in an ICO: The Importance of Vesting to Align Incentives, Steemit (2017), https://steemit.com/blockchain/@dana-edwards/criteria-for-determining-fair-distribution-in-an-ico-the-importance-of-vesting-to-align-incentives?sort=new [https://perma.cc/3X6C-CANT].

105. See, e.g., Kaplan & Strömberg, supra note 94, at 292 ("VC financings commonly utilize both founder vesting and non-compete clauses.")

106. We did not observe any of the tokens in our sample using an options mechanism. Anecdotally, we are only aware of one project that has used options to facilitate development: Ripple. See Anna Irrera, U.S. Blockchain Startups R3 and Ripple in Legal Battle, Reuters (Sept. 8, 2017), https://www.reuters.com/article/us-r3-ripple-lawsuit/u-s-blockchain-startups-r3-and-ripple-in-legal-battle-idUSKCN1BJ27I [https://perma.cc/W64R-Z7NR]. Perhaps one reason that options mechanisms are underrepresented is that appropriate strike prices are hard to determine for tokens. See Editorial Team, CryptoCurrency Options—An Alternative Way to Trade Crypto, CoinBureau (Aug. 22, 2018), https://www.coinbureau.com/education/cryptocurrency-options/ [https://perma.cc/ZF94-FBQS] (detailing the volatility of Bitcoin's strike prices).

107. Bancor, Bancor Network Token (BNT) Contribution & Token Allocation Terms, Medium (June 5, 2017), https://medium.com/@bancor/bancor-network-token-bnt-contribution-token-creation-terms-48cc85a63812 [https://perma.cc/VR97-EL2Y].

108. Luis Cuende, Aragon Network Token Sale Terms: Founder Vesting, Simple Pricing and Distribution, Aragon One Blog (Apr. 21, 2017), https://blog.aragon.one/aragon-network-token-sale-terms-8998f63a3429 [https://perma.cc/G7X6-7WQC].

109. See supra note 6 and accompanying text.

110. As an example, consider NaPoleonX, which changed its vesting mechanism from six months to a series of four distribution periods halfway through its ICO process. See Stéphane Ifrah, NaPoleonX Newsletter, NaPoleonX, http://notifications.napoleonx.ai/napoleonx-update-31/01 [https://perma.cc/S4YA-M9YP] (last visited Feb. 4, 2019).

employment contracts of the various managers and founders, but such contracts probably will not be publicly verifiable.

Perhaps to allay this very concern, ICOs often make claims about their smart contract vesting. For instance, one promises that:

> 20% of the BMCs will be allocated to the founding Blackmoon Crypto team and advisors, locked in a smart contract with a 24-month vesting period, and six-month cliff. These BMCs won't be immediately tradable and will secure the core team members by ensuring their motivation after the Distribution Period.[111]

Because promoters focus on it so much, examining how and whether vesting promises are coded sheds light on how strongly investors should buy the claim that a project's key people will not exit with their newly raised capital.[112] That is not to say that failing to code vesting means that founders are about to abscond: Coded vesting rules are only one way to protect against looting. However, it is a way that is technically feasible and consonant with the industry's ideological claim that law is a poor substitute for code.

A third and final protection against exploitation in ICOland is the supposition that the initial rights investors receive are not modifiable. Part of the appeal of cryptoassets and smart contracts that operate on blockchains hinges on their "immutable" nature. Legal contracts contain ambiguity and permit formal and informal modifications, but smart contracts are purportedly drafted in exhaustive, precise code that seems to set the parties' obligations permanently.[113] Because cryptoassets are defined by smart contracts, whether those smart contracts are modifiable should profoundly impact price and receive intense investor scrutiny.[114]

A fully disclosed regime that permitted a token to be modifiable should have uncertain effects on value. On the one hand, no social enterprise

---

111. Blockchain Paper, Black Moon Investment Analysis: Blackmoon Crypto, Medium (Sept. 7, 2017), https://medium.com/@researchpaper/blackmoon-crypto-is-part-of-the-blackmoon-financial-group-a-financial-technology-company-founded-56b5a64d88c3 [https://perma.cc/M3V6-BFBC].

112. The story of a project called Matchpool demonstrates how the absence of coded vesting rules can result in mischief. Within days of a reported $5.7 million ICO, one founder departed from the project and wrote that his cofounder, the CEO, had withdrawn 37,500 ether from the wallet without explanation. See Nick Tomaino (@NTmoney), Twitter (Apr. 5, 2017), https://twitter.com/NTmoney/status/849755116156600321 [https://perma.cc/RXE2-NNUQ].

113. See Sklaroff, supra note 49, at 291.

114. In fact, to the extent that investors are told to focus on code, they are explicitly warned that it will be immutable. See, e.g., Catalin Cimpanu, Researchers: Last Year's ICOs Had Five Security Vulnerabilities on Average, Bleeping Comput. (June 25, 2018), https://www.bleepingcomputer.com/news/security/researchers-last-year-s-icos-had-five-security-vulnerabilities-on-average/ [https://perma.cc/DRW3-99RN] ("Once an ICO starts, the contract cannot be changed and is open to everyone, meaning anyone can view it and look for flaws." (internal quotation marks omitted) (quoting Positive ICO, ICO Projects Contain Five Security Vulnerabilities on Average, Positive.com Blog (June 25, 2018), https://blog.positive.com/positive-com-ico-projects-contain-five-security-vulnerabilities-on-average-a6c6a818d89a [https://perma.cc/A3XC-N4AR])).

existing over any medium-length time period can have functioning governance rules immutably fixed at its inception. Human relations, including financial ones, evolve. Imagine a constitution that could never be amended, or a similar corporate charter.[115] Thus, investors told that every rule of a token ecosystem had been irrevocably fixed at their creation should (we think) recoil at the coders' hubris.[116] On the other hand, when one party holds the power to modify formal relations, other parties bear risk. To the extent that a smart contract defining investors' rights is mutable at the will of the issuer, investors ought to expect that the limits of that process would be explained in detail. Consider a fully modifiable Colacoin, for instance. One day the issuer might say that your coin, which you thought bought you a right to delicious fizzy soda, could only be used to purchase noncarbonated beverages or could be used to purchase cola only when you inserted additional fiat currency.[117] The "rights" you bought would be notional.

Surprisingly, until July 2018, the crypto industry rarely discussed modification.[118] That month, in response to a hack of a popular token, a handful of prominent cryptocurrency voices sounded the alarm that several circulating tokens were modifiable at will.[119] They were, to summarize a long Twitter thread, angry. This is not conclusive evidence that modifiability is seen as a negative characteristic of tokens, but it does suggest that the coded ability to modify a token is not an anodyne fact. In short: We would expect that if token code is explicitly modifiable, that fact would be disclosed. Similarly, if the token code's governance provisions are not modifiable, we would expect that the marketing

---

115. Cf. Henry Hansmann, Corporation and Contract, 8 Am. L. & Econ. Rev. 1, 2 (2006) (suggesting that corporations adopt state-law default terms for their charters in order to delegate a long-term amendment power to their states of incorporation).

116. See Sklaroff, supra note 49, at 300 (providing instances of that hubris meeting its just reward).

117. There are parallels between freely modifiable tokens and blank check stock, which gave rise to significant concerns immediately before the SEC was chartered. See generally Harwell Wells, A Long View of Shareholder Power: From the Antebellum Corporation to the Twenty-First Century, 67 Fla. L. Rev. 1033, 1071 (2015) (discussing Adolf A. Berle Jr. & Gardiner C. Means' historic critique of "blank check stock" for permitting board entrenchment).

118. Earlier discussions did exist but were limited to blog posts and commentary outside of the mainstream. See, e.g., Alan Lu, Solidity DelegateProxy Contracts, Gnosis (May 17, 2018), https://blog.gnosis.pm/solidity-delegateproxy-contracts-e09957d0f201 [https://perma.cc/ZVN8-6UP8] ("Proxies can enable contract logic to be updatable as well, so additional business requirements may be implemented after the initial deployment. Of course, this is a tradeoff: contract users would have to trust that the contract owner updates the contract in a way that does not violate user expectations.").

119. See Jackson Palmer (@ummjackson), Twitter (July 9, 2018), https://twitter.com/ummjackson/status/1016455890294091776 [https://perma.cc/WKG8-WDL9] (identifying that some tokens "include an 'upgrade' capability which also allows them to essentially upgrade/replace the token contract" and others allow token creators have the "to completely and centrally pause transfers").

documents would explain how, and why, the project can evolve with the times.

With these three investor-protection ideas in hand, we now will provide examples of how they are actually accomplished in the real world. We focus our discussion on Ethereum code. Ethereum nodes operate a simulated computer called the "Ethereum Virtual Machine" (EVM).[120] This simulation runs by using both data and code (smart contracts) stored on the Ethereum ledger.[121] The smart contracts exist on the Ethereum ledger in a complex, hard-to-read machine language known as bytecode.[122] But they are most commonly written in an intuitive programming language called Solidity.[123] Solidity hides the internal details of the EVM and the complex machine language that it processes.[124] Before being uploaded to the blockchain, a program called a compiler is used to translate the Solidity source code into Ethereum bytecode.[125] This Article presents examples in Solidity.

Solidity code contains four major types of entities: variables, functions, events, and modifiers.[126]

- *Variables* are the data-storage components of any smart contract and, in the case of a token's smart contract, store balances for each user-address, along with other data required for the smart contract to operate.[127]
- *Functions* describe the rules by which the smart contract operates, storing discrete chunks of code that perform specific tasks.[128] Functions are executed (or "called") by sending a specially formatted transaction to the Ethereum network.[129] Functions are identified by a name and a set of parameters (or "arguments") that are the inputs to the function.[130]

---

120. What Is Ethereum?, Ethereum Homestead Documentation, http://ethdocs.org/en/latest/introduction/what-is-ethereum.html [https://perma.cc/53WA-DANP] (last visited Jan. 26, 2019).

121. Id.

122. See Bernard Peh, Solidity Bytecode and Opcode Basics, Medium (Sept. 15, 2017), https://medium.com/@blockchain101/solidity-bytecode-and-opcode-basics-672e9b1a88c2 [https://perma.cc/ZDB3-BH7P].

123. See id. ("Like many other popular programming languages, Solidity is a high level programming language.").

124. Id.

125. Id.

126. Structure of a Contract, Solidity, https://solidity.readthedocs.io/en/v0.5.2/structure-of-a-contract.html [https://perma.cc/UD2K-3WDZ] (last visited Jan. 26, 2019).

127. Id.

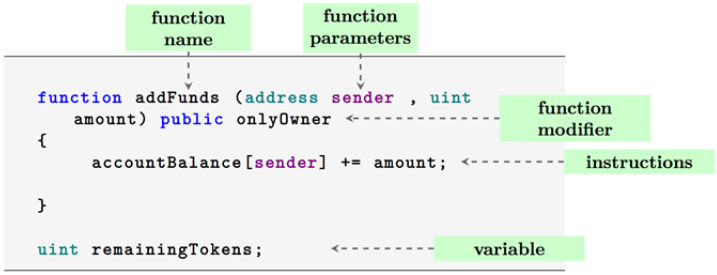
128. Id.

129. Id.

130. Id.

- *Events* are signals that a smart contract sends to other applications or smart contracts programmed to receive them.[131] They act as a form of logging.[132]
- *Modifiers* allow a developer to easily restrict the execution of a function under certain conditions.[133] For example, a developer may restrict the ability to mint new tokens to the smart contract owner alone.[134]

FIGURE 4: AN EXAMPLE CODE SNIPPET[135]



To audit a given cryptoasset, we obtain a copy of the Solidity code (illustrated above), either from etherscan.io, where developers commonly upload their smart contract's Solidity code, or from GitHub, a source code repository often used as part of the development process. Etherscan.io replicates the bytecode present on the blockchain but requires developers to upload Solidity source code for display.[136] The site

131. Id.

132. See Contracts, Solidity, https://solidity.readthedocs.io/en/v0.5.2/contracts.html [https://perma.cc/845Q-9DEG] (last visited Jan. 26, 2019) ("Solidity events give an abstraction on top of the EVM's logging functionality.").

133. Id.

134. See id.

135. The code snippet shows a fictional "addFunds" function that adds funds to the sender's account balance. The code can only be executed by the contract owner, as indicated by the "function modifier." To execute the function, a user must supply two parameters: (1) the address of the sender and (2) the amount by which to increase the account balance—these are commonly known as "arguments." The operator "+=" then adds the variable "amount" to the variable "accountBalance[sender]" and then saves that new value as the variable "accountBalance[sender]."

136. See Contract Verification - Constructor Arguments, Etherscan Support Ctr., https://etherscancom.freshdesk.com/support/solutions/articles/35000022165-contract-verification-constructor-arguments [https://perma.cc/2FTU-86WD] (last updated Nov. 21, 2017); What Is Etherscan?, Etherscan Support Ctr., https://etherscancom.freshdesk.com/support/solutions/articles/35000022140-what-is-etherscan [https://perma.cc/KD78-SSBS] (last updated Nov. 21, 2017).

additionally provides a verification feature, which allows users to check that the Solidity code matches the bytecode.[137]

After obtaining source code, we then examine each function of a smart contract and manually track the role each line plays. We use code comments—explanatory lines of human-language text inserted by developers, which have no computational function—as guides to assist in identifying developers' intentions.[138] A typical smart contract in our sample contains between five hundred and one thousand lines of code. We inspect that code, looking for the presence of our three investor-protection attributes.

A. *Supply Promises*

1. *Minting.* — Cryptoassets issued via ICOs are created through a process known as minting.[139] Recall that the Ethereum blockchain provides an extremely simple way to mint new cryptoassets through the ERC-20 standard.[140] But even if they do not conform to the ERC-20

---

137. See Contract Verification - Constructor Arguments, supra note 136. In a few cases, Etherscan did not affirmatively indicate that the uploaded display code matched the bytecode. In those cases, we did not separately verify the match.

138. Importantly, our assessment does not constitute a security audit, nor does it guarantee the correctness of the code. It merely seeks to ascertain the intended purpose of the various contract components. We leave analyzing the correctness of ICO smart contracts to others. Source code can be examined along a number of axes, among them syntax, semantics, and correctness. Syntax refers to the symbolic representation of the code—the particular sequence of words and numbers that comprise code. See Richard Paige, Foundations of Tree- and Graph-Based Abstract Syntax *in* Software Languages: Syntax, Semantics, and Metaprogramming 87, 87 (Ralf Lämmel ed., 2018). In our case, this is the set of rules governing the Solidity language. At a higher level of abstraction, the semantics of code refers to the actual meaning or functionality of a program. Isabelle Attali, A Primer on Operational Semantics *in* Software Languages: Syntax, Semantics, and Metaprogramming, supra, at 241, 241. Therefore, two pieces of code written in different programming languages can have the same semantics, while differing in syntax. As a result, semantics is the level at which we attempt to audit the code.

139. See David Hoffman, Penn Wharton Pub. Policy Initiative, Regulating Initial Coin Offerings (ICOs) 2 n.2 (2018), https://publicpolicy.wharton.upenn.edu/live/files/303-a [https://perma.cc/W5TW-K2AP]. An alternative process, known as mining, is often used to create cryptoassets, but not for ICOs. See Böhme et al., supra note 38, at 222 ("[B]itcoins are created when a miner successfully solves a mathematical puzzle."). In mining, suppliers of computational power receive cryptoassets in exchange for performing network-critical functions for the blockchains housing the cryptoassets. Id. at 218. Bitcoin provides an archetypal example of mining. Id. Bitcoin miners devote processing power to the blockchain, using their computers to solve complex math problems that help verify transactions. Id. The first miner to discover a valid solution can lay claim to the newly mined bitcoin. Id. For further details, see id. at 215–18.

140. See Hoffman, supra note 139, at 2; see also supra text accompanying notes 55–58. Using instructions found online, we were able to mint our own cryptoasset in twenty minutes. See maxnachamkin, How to Create Your Own Ethereum Token in an Hour (ERC20 + Verified), Steemit (July 10, 2017), https://steemit.com/ethereum/@maxnachamkin/How-to-create-your-own-ethereum-token-in-an-hour-erc20-verified [https://perma.cc/A5U5-RDK7].

standard, minted assets are typically created by executing relatively simple code on a blockchain.[141]

In other words, a minted cryptoasset is created through an act of founder fiat. Billions or trillions of cryptoasset tokens are generated at a nominal cost reflecting fees paid to interact with the respective blockchain.[142] Then the team will typically commence an ICO, transferring the tokens to investors in private sales or to members of the general public in mass offerings. The sales are accomplished using smart contracts, automatically routing the project's tokens to investors in exchange for other cryptoassets or, more rarely, for fiat currency.

Minting is an essential part of the ICO story. It creates the opportunity for early-stage blockchain projects to rapidly raise capital without the formalities required by corporate law and regulation. But it also opens the door to fraudsters, who can mint and sell tokens based on the expectation of a given supply schedule, only to mint more than expected—or to mint a special stash for themselves.

To understand minting, let's examine an ICO for a cryptoasset called Kin (ticker symbol: KIN), orchestrated by a company called Kik Interactive ("Kik"). Kik runs a global messaging platform with approximately 300 million registered users.[143] Like other digital communications companies, it has sought to broaden its business model by turning to blockchain.[144] Ultimately the company would like to build a "decentralized ecosystem of digital services for daily life."[145]

If all goes according to plan, Kin will be the currency enabling and constituting this utopian ecosystem.[146] Building on Kik's previous efforts to develop in-app loyalty points, Kin is meant to serve as a "transaction currency" that Kik users can exchange for premium features, like

---

141. This is not a necessary attribute of minted assets. For a summary of the smart contract code audited, see infra notes 594–645.

142. In our sample, some teams minted the full supply of their cryptoasset instantaneously. Others chose a dynamic supply model, in which supply grew proportionately to the amount of investment received.

143. Lucas Matney, Kik Already Has Over 6,000 Bots Reaching 300 Million Registered Users, TechCrunch (May 11, 2016), https://techcrunch.com/2016/05/11/kik-already-has-over-6000-bots-reaching-300-million-registered-users/ [https://perma.cc/GYN7-LAAD].

144. Kik Interactive, Inc., Kin: A Decentralized Ecosystem of Digital Services for Daily Life 3 (2017), https://kinecosystem.org/static/files/Kin_Whitepaper_V1_English.pdf [https://perma.cc/V3QE-ZHNF] [hereinafter Kik Interactive, Kin: A Decentralized Ecosystem] (advocating for the adoption of blockchain-based networks to facilitate digital ecosystems in order "to realize Kik's vision of a sustainable future in online communication and commerce").

145. Id.

146. See id. at 23 ("Kin will bring to fruition a new era of decentralized community ownership, enabling a vibrant ecosystem of digital services that power daily life.").

membership in "VIP" chat groups with celebrities.[147] It will also incentivize developers to work alongside the project.[148]

According to its whitepaper, Kik planned to mint ten trillion Kin tokens, of which one trillion would be put up for sale.[149] A blog post from Kik's founder and CEO states that 488 billion were sold for $50 million in a presale arranged with specific investors and venture capital funds active in the industry.[150] The remaining 512 billion tokens were offered to the public during the project's ICO, which ran from September 12–26, 2017.[151] Ultimately, the ICO raised $98.8 million for the project, bringing the total amount raised to almost $150 million when including the private presale.[152]

We audited the smart contract code to understand how these supply promises were accomplished. The cap on the number of tokens available is indeed coded in the smart contract. In addition, the smart contract mandates two discrete sale phases, and there are coded limits on how many tokens could be sold during each. One of these phases is the project's ICO, and the other is presumably the private presale.[153] Figure 5 illustrates the code's function.

---

147. Id. at 5, 13–15. Other proposed premium features include the ability to publish messages with special visual features or to broadcast "shoutout" messages to large groups. Id.

148. See id. at 5–6, 19 (describing how a "Kin Rewards Engine" will "create natural incentives for digital service providers to adopt Kin and become partners in the ecosystem").

149. Id. at 21.

150. Ted Livingston, Kin TDE: If You Want to Participate, You *Must* Register by September 9, 9:00 a.m. ET, Medium (Aug. 29, 2017), https://medium.com/kinfoundation/kin-tde-if-you-want-to-participate-you-must-register-by-september-9-9-00-a-m-et-2f1304a4aa4b [https://perma.cc/2RMJ-FREH]; see also Khari Johnson, Kik Raises $50 Million Ahead of Token Sale for Its Cryptocurrency Kin, VentureBeat (Aug. 29, 2017), https://venturebeat.com/2017/08/29/kik-raises-50-million-ahead-of-token-sale-for-its-cryptocurrency-kin/ [https://perma.cc/3DRF-NRZL] ("Presale investors include Blockchain Capital, Pantera Capital, and Polychain Capital, all well-known blockchain-specific investment firms.").

151. See Khari Johnson, Kik Raises $98 Million in Kin Cryptocurrency Token Sale, VentureBeat (Sept. 26, 2017), https://venturebeat.com/2017/09/26/kik-raises-98-million-in-kin-cryptocurrency-token-sale/ [https://perma.cc/Q9WU-PAR2] [hereinafter Johnson, Kik Raises $98 Million]; Kin Token Distribution Event Starts Today, Kik Blog (Sept. 12, 2017), https://www.kik.com/blog/kin-token-distribution-event-starts-today/ [https://perma.cc/M7Z6-GA7Q].

152. See Johnson, Kik Raises $98 Million, supra note 151. Due to concerns that there would be insufficient demand to sell the entire ICO stake, Kik ended the sale eight hours earlier than initially planned, and announced that it would distribute all unsold tokens to ICO buyers on a pro-rata basis. See u/masrod, Maintaining the Kin Token Structure: Redistributing Unsold Kin, r/KinFoundation, Reddit (Sept. 24, 2017), https://www.reddit.com/r/KinFoundation/comments/724xg9/maintaining_the_kin_token_structure/ [https://perma.cc/YU9X-8AZE].

153. To purchase tokens, purchaser addresses must be added to a list of participants by Kin's development team. See Livingston, supra note 150.

FIGURE 5: KIN PROJECT CODE[154]

```
uint256 public constant MAX_TOKENS = 10 ** 13 * TOKEN_UNIT;
uint256 public constant MAX_TOKENS_SOLD = 512195121951 *
    TOKEN_UNIT;
uint256 public constant WEI_PER_USD = uint256(1 ether) /
    289;
uint256 public constant KIN_PER_USD = 6829 * TOKEN_UNIT;
uint256 public hardParticipationCap = 4393 * WEI_PER_USD;

function create(address _recipient) public payable
    onlyDuringSale {
    require(_recipient != address(0));

    uint256 weiAlreadyParticipated =
        participationHistory[msg.sender];
    uint256 participationCap =
        SafeMath.min256(participationCaps[msg.sender],
        hardParticipationCap);
    uint256 cappedWeiReceived = SafeMath.min256(msg.value,
        participationCap.sub(weiAlreadyParticipated));
    require(cappedWeiReceived > 0);

    uint256 weiLeftInSale =
        MAX_TOKENS_SOLD.sub(tokensSold).
      div(KIN_PER_WEI);
    uint256 weiToParticipate =
        SafeMath.min256(cappedWeiReceived, weiLeftInSale);
    participationHistory[msg.sender] =
        weiAlreadyParticipated.add(weiToParticipate);
    fundingRecipient.transfer(weiToParticipate);

    // CODE REMOVED FOR BREVITY

    tokensSold = tokensSold.add(tokensToIssue);
    issueTokens(_recipient, tokensToIssue);

    uint256 refund = msg.value.sub(weiToParticipate);
    if (refund > 0) {
        msg.sender.transfer(refund);
    }
}
```

Here, the developers hard-code a number of values for use in later functions.

Here and elsewhere we removed both variables and code to better suit our presentation format, while retaining key features.

The "create" function is run each time ether is transferred to the contract during the ICO—set at 14 days from creation.

The final function checks that neither the individual nor the total caps have been reached and then mints and issues to the sender the appropriate amount of Kin—stored within the contract's ledger.

That is minting. But there are other processes that can alter supply.

2. *Increasing Supply.* — The full supply of a minted cryptoasset can be set at the outset of a project, or can fluctuate depending on how much investment the project receives.[155] The circulating supply of the asset can also fluctuate. For instance, a founding team could retain some of an initially minted asset supply and use it to inflate the circulating amount in the future.[156] Similarly, a team might alter rules governing the

154. Kin (KIN), Contract Code, Etherscan, https://etherscan.io/address/0x818fc6c2ec5986bc6e2cbf00939d90556ab12ce5#code [https://perma.cc/5CUF-SFC6] (last visited Feb. 20, 2019).

155. See supra Figure 5 (setting the max tokens in the first two lines of code).

156. See, e.g, Brad Garlinghouse, Ripple to Place 55 Billion XRP in Escrow to Ensure Certainty of Total XRP Supply, Ripple, https://ripple.com/insights/ripple-to-place-55-billion-xrp-in-escrow-to-ensure-certainty-into-total-xrp-supply/ [https://perma.cc/8FWS-FP5M] (last visited Jan. 26, 2019) (explaining Ripple's decision to place 55 billion XRP into a "cryptographically-secured escrow account" to secure XRP).

ICO process to achieve various supply effects. For example, the Kin ICO smart contract contains code to enforce volume restrictions for individual purchasers.[157] Each address permitted to participate in the sales may only send a limited amount of ether to the smart contract that disburses KIN tokens.[158] However, these limits could be manually modified by the smart contract owner at any time.[159]

The important point here is that maximum supply of a minted cryptoasset can be specified and enforced (or not) via the code comprising the cryptoasset itself. Projects can also contain an absolute cap. But some cryptoassets lack this feature. For example, there is no absolute cap on the amount of ether that can be created.[160] Indeed, there is heated debate about whether this is a desirable feature or not.[161]

Supply caps are a typical part of an ICO's marketing materials.[162] As one promoter said, "Even if on the last day of distribution Richard Branson shows up on a resplendent white yacht packed stern to bow with cash, we wouldn't be able to sell him any more."[163]

3. *Decreasing Supply (or "Burning").* — In prototypical blockchains, cryptoassets circulate like money. Think of Colacoin: If you drop a Colacoin in a vending machine for a pop, the coin will get picked up by a Coca-Cola employee, head to the corporate vault, be used in payment for the vault guard's salary, and then—maybe after the vault guard goes for a jog—get dropped back into another vending machine in the system. To take one example, circulation is the default rule for ether.[164] When

157. See supra Figure 5 (comparing weiAlreadyParticipated, the number of tokens already purchased, with participationCap, the total amount allowed to be purchased, and msg.value, which contains the requested purchase amount).

158. See supra Figure 5 (creating a cap on ether received).

159. This structure creates opportunities for the development team to temporarily increase caps and quietly notify certain favored purchasers, and then reduce the cap once the additional purchases have been made. See Kin (KIN), supra note 154 (providing several means to place participants in different tiers with different caps).

160. See Ether, Ethereum, https://www.ethereum.org/ether [https://perma.cc/39TF-TDR6] (last visited Jan. 26, 2019).

161. See Michael Collins, Ethereum Stakeholders Consider Capping the Amount of Total Ether, Bitrates (Aug. 26, 2018), https://www.bitrates.com/news/p/ethereum-stakeholders-consider-capping-the-amount-of-total-ether [https://perma.cc/MYY6-BC26] (discussing proposals to cap the amount of ether). Despite many attempts to impose a hard cap, there has been no progress. See Vitalik Buterin (@VitalikButerin), Twitter (Apr. 2, 2018), https://twitter.com/VitalikButerin/status/980744740277661696 [https://perma.cc/Q7SX-SBZF] (describing an April Fool's joke proposing implementing a currency cap on ether and therefore demonstrating that there is still no cap). Note that ether supply is in some ways determined by the economics of mining, a reference to the "ice age" difficulty bomb. See Collins, supra.

162. See infra Part III & Appendix B.

163. See dennisk82, Polybius Bank (PLBT Tokens), Steemit (July 12, 2017), https://steemit.com/crypto/@dennisk82/polybius-bank-plbt-tokens [https://perma.cc/TS9B-C2NY].

164. See Ethereum Whitepaper, supra note 48.

someone pays ether to complete a transaction on the Ethereum blockchain, its recipient can spend that ether right away.[165]

But perpetual circulation is not always the fate of a cryptoasset. Cryptoassets also can be used up, or "burned"—that is, destroyed.[166] Burning can play important roles depending on the business model envisioned by project founders. Some might advertise that the token could be exchanged for the right to access the completed project. Then, the exchanged asset would be permanently "burned" upon use. Some projects described plans to actively buy tokens from holders and then burn them, creating token price appreciation similar to a stock buyback.[167] In others, only those tokens exchanged for certain features in the product—for example, tokens paid as fees—are burned. Finally, burning is used as a mechanism in ICOs, as a way to destroy unsold supply.

Burning on the Ethereum blockchain takes two forms. The first is a simple transfer of tokens (or ether) to the address of Ethereum's "genesis" block,[168] consisting of all zeros. As this address has no owner, the tokens cannot be spent and as such are "burned." The second is to use an Ethereum smart contract's function programmed with the logic to either delete the ownership record and decrement the total supply accordingly, or that which destroys the entire smart contract, rendering

---

165. See id.

166. See Natale M. Ferrara, 'Token Burning' and Other Crypto Jargon Simplified, Forbes (Nov. 29, 2017), https://www.forbes.com/sites/eidoo/2017/11/29/token-burning-and-other-crypto-jargon-simplified/ [https://perma.cc/V323-SYF2] ("In its simplest form, burning a token means making the token permanently unspendable.").

167. See, e.g., FinShi Capital Crowdsale Whitepaper, FinShi Capital, http://finshi.capital/whitepaper_finshi_eng.pdf [https://perma.cc/WEZ9-27WX] (last visited Jan. 26, 2019). FinShi's whitepaper states:

> FinShi Capital takes on the obligation of buying back the tokens through the fund's profits, thus implementing dividend policy. Once the fund announces an exit from a portfolio company, there will be created a queue of investors who applied for selling their tokens back to the fund. The amount of tokens for buy-back will be announced together with the exit date. The fund will buy out the tokens within one month after the exit from a startup. After that the tokens will be destroyed.

Id. As Professor Tony Casey pointed out to us, the economics of buy-backs are interesting in that the functional result is to distribute residual profits to nonowners. Presumably, the organizers have concluded that such commitments, whether or not credible, can result in a more profitable immediate liquidity event, suggesting that they discount the possibility of long-term gains.

168. Every entry ("block") on a blockchain is linked to both the entry following it and the entry preceding it. However, this cannot apply to the first block which has no antecedent. This block, known as the "genesis block," is created by computer code explicitly laying out the contents of the ledger entry. See Genesis Block, Bitcoin Wiki, https://en.bitcoinwiki.org/wiki/Genesis_block [https://perma.cc/SDR2-UYH5] (last visited Jan. 26, 2019).

any tokens or ether sent to that address inaccessible. The below snippet shows a characteristic burning function.

FIGURE 6: BURNING CODE[169]

```
function burn(uint256 _value) public returns (bool
    success) {
    require(balanceOf[msg.sender] >= _value);

    balanceOf[msg.sender] -= _value;
    totalSupply -= _value;

    Burn(msg.sender, _value);
    return true;
}
```

A smart contract with appropriate code can keep track of burned tokens, enabling investors to easily audit the current supply.

Not all burning promises are executed so cleanly. Consider, for instance, Paragon, an ICO that aims to "revolutioniz[e] all things cannabis with blockchain."[170] Lest you think it's all a smoky haze (and we promise that's the first and last joke), the project does have a dedicated cryptoasset: an ERC-20 token called PRG. The whitepaper specifies that PRG holders will be able to interact with all of the project's many initiatives; holders will be able to vote on real estate investments,[171] guide project governance decisions,[172] purchase access to coworking services,[173] and exchange tokens for local currency in cannabis-unfriendly jurisdictions.[174]

---

169. The burning code checks that the user has a sufficient balance of tokens, reduces their account balance and total supply by the request amount, and notifies interested parties through the "Burn" event. See Create Your Own Crypto-Currency with Ethereum, Ethereum, https://www.ethereum.org/token [https://perma.cc/NC6X-NED2] (last visited Feb, 21, 2019).

170. Paragon, Whitepaper Version 1.0, at 1 (2017), https://paragoncoin.com/whitepaper.pdf [https://perma.cc/5K5W-9SWH]. "All things" is not really an exaggeration; the whitepaper discusses plans to streamline operations for cannabis growers and dispensaries, purchase and operate coworking spaces for cannabis startups, and engage in widespread prolegalization advocacy. Id. The whitepaper describes a ParagonSpace, a Paragon Accelerator, an "immutable ledger for all industry related data." Id. at 8. Of course, all of these efforts are powered by cryptoassets and smart contracts.

171. See id. at 21.

172. See id.

173. See id. at 17–18.

174. See id. at 12. Ultimately, the SEC focused on these promises when it brought a cease-and-desist action against the Paragon team for selling unregistered securities. See In re Paragon Coin, Inc., Securities Act Release No. 10574, 2018 WL 6017663, at *4 (Nov. 16, 2018) (noting that "Paragon and its agents . . . emphasized that the company would build an 'ecosystem' in a way that would cause PRG tokens to rise in value"). This has been one of the highest-profile enforcement actions against ICO teams; many have suggested that it was the nail in the coffin for the 2017–2018 ICO market. See Nikhilesh De, After Friday's SEC Actions, Experts Say ICO Party 'Is Truly Over,' CoinDesk (Nov. 17, 2018),

In addition to these promises about governance, Paragon promised that any unsold tokens from the private or public sale would be burned.[175] And it describes a transaction fee system whereby "[a]ll fees on the Paragon ecosystem" incur a $0.000000005 charge (that's five billionths of a dollar), half of which is burned and half of which replenishes the project's PRG reserve.[176]

We can perceive only a small part of this complex set of rules in the code.[177] PRG's smart contract code does limit issuance to 200 trillion tokens. This is captured in Figure 7 below.

FIGURE 7: PARAGON SUPPLY CODE[178]

```
uint256 constant INITIAL_TOKENS_COUNT = 200000000e6;

function ParagonCoinToken (address fundAddress) {
  tokensCount = INITIAL_TOKENS_COUNT;
  accounts [msg.sender] = INITIAL_TOKENS_COUNT;
  owner = msg.sender;
  fund = fundAddress;
}

function name () constant returns (string name) {
  return "PRG";
}

function symbol () constant returns (string symbol) {
  return "PRG";
}
```

The code that is unique to PRG consists mostly of variables specifying the name of the token and quantity of tokens available.

We also verified that Paragon contains code allowing users to burn a portion of their tokens. This is captured in Figure 8 below.

---

https://www.coindesk.com/after-fridays-sec-actions-experts-say-ico-party-is-truly-over [https://perma.cc/F94J-BA6K] (suggesting that due to enforcement actions against Paragon and other ICO projects, "the party is truly over").

175. See Paragon, supra note 170, at 14.

176. Id. at 32. Finally, the whitepaper describes a process for stabilizing the price of PRG by selling or buying back tokens. This suggests that the team can unilaterally change the number of tokens in circulation when it deems that that there is "severe price volatility" or "excessive sell volume," making it difficult for investors to value tokens ex ante. Id. at 31. The project does claim that Reserve Funds "cannot be . . . distributed to employees or investors," and that insiders are restricted from trading PRG following a purchase or sale by the Fund, though there is no enforcement mechanism specified. Id.

177. The Paragon code repository contains what appears to be a third-party audit certification by ABDK Consulting, a blockchain services consultancy. The certificate claims that the auditors have inspected the code and "the code does not contain any major flaws that would prevent a secure and proper interaction with this contract." Mikhail Vladimirov & Dmitry Khovratovich, ABDK, ParagonCoin Token Contract: Final Report, Github (Sept. 15, 2017), https://github.com/paragon-coin/token/blob/master/ParagonCoinTokenContractFinalReport.pdf [https://perma.cc/QNC3-QBFY]. The auditors also noted that "the contract charges a fee . . . which should be made clear." Id.

178. Paragon (PRG), Contract Code, Etherscan, https://etherscan.io/address/0x7728dFEF5aBd468669EB7f9b48A7f70a501eD29D#code [https://perma.cc/F58F-M3G4] (last visited Feb. 16, 2019).

FIGURE 8: PARAGON COIN BURNING CODE[179]

```
// BURN GIVEN NUMBER OF TOKENS BELONGING TO MESSAGE
    SENDER
function burnTokens (uint256 _value) returns (bool
    success) {
  if (_value > accounts [msg.sender]) return false;
  else if (_value > 0) {
    accounts [msg.sender] = safeSub (accounts
        [msg.sender], _value);
    tokensCount = safeSub (tokensCount, _value);
    return true;
  } else return true;
}
```

PRG here provides a facility for burning tokens in a manner that registers a decrease in the token supply.

However, we modeled the transaction fee system described in the paper and discovered troubling implications for supply. Following the creation of the smart contract, each transfer of a PRG token consumes approximately one-six-billionth of the total supply in transfer fees, half of which is paid to the owner of the PRG smart contract and half of which is burned. After a sufficient number of transactions the fee approaches the number of tokens remaining in the supply, causing the eventual demise of the network. This is captured in Figure 9 below.

FIGURE 9: PARAGON FEE CODE[180]

```
function fee() constant returns (uint256) {
    return safeAdd(safeMul(tokensCount, 5)/1e11, 25000);
}

function processFee(uint256 feeTotal) internal returns
    (bool) {
    uint256 burnFee = feeTotal/2;
    uint256 fundFee = safeSub(feeTotal, burnFee);

    accounts [fund] = safeAdd(accounts [fund], fundFee);
    tokensCount = safeSub(tokensCount, burnFee);

    Transfer (msg.sender, fund, fundFee);
    return true;
}
```

Each PRG transactions is accompanied by a token fee of *supply* * 5 * 10^{-33} + 2500.

Half of these tokens are permanently removed from the supply, and half are distributed to the owner.

Eventually, this leads to a complete depletion of the token supply.

B. *Vesting Promises*

If supply controls protect against the threat of dilution, vesting mechanisms protect against the threat of desertion.[181] They work either by delaying when the founder is granted assets or deferring the moment of their liquidity.[182] A smart contract usually provides for vesting by allocating a portion of minted tokens to insiders but then locking them

179. Id.

180. Id.

181. See supra note 104 and accompanying text.

182. See, e.g., Kin (KIN), supra note 154 (granting assets that vest periodically over different periods).

up until some condition is satisfied.[183] The code prohibits the transfer, sale, or use of the tokens until the condition's trip-wire is hit.[184] Most ICO-coded vesting is time-based, with few of the contractual conditions that come with stock vesting offline.[185]

Let's return to Kik and examine its vesting promises. In its marketing documents, Kik made fairly specific, detailed promises about token vesting. Of the ten trillion total Kin created, Kik's whitepaper claimed that thirty percent would be allocated to Kik in exchange for its "startup resources, technology, and a covenant to integrate with the Kin cryptocurrency and brand."[186] This stake would be subject to a vesting schedule that released ten percent every quarter, for ten quarters.[187]

Further, sixty percent of the initial Kin was allocated to the Kin Foundation, the entity that is meant to gradually take control of the project.[188] This stake vests according to its own schedule.[189] A total of 0.061% of this stake will be released into circulation daily, or roughly twenty percent per year.[190] Kik even released a separate whitepaper detailing the vesting dynamics for the Foundation stake, specifying, for example, that the unvested portion of this stake will be around 4.6 trillion Kin on March 12, 2019.[191]

---

183. See, e.g., StatusNetwork (SNT), Contract Code, Etherscan, https://etherscan.io/address/0x744d70fdbe2ba4cf95131626614a1763df805b9e#code [https://perma.cc/FG4X-DRXM] (last visited Feb. 16, 2019) (granting tokens to a holding wallet where they are collectable after they vest).

184. The team could always choose to mint new tokens not subject to the vesting condition and claim that the project will eventually accept both kinds of tokens.

185. There are, of course, outliers. Aragon, an Ethereum-based platform for building and managing decentralized organizations, claimed that its ERC-20 tokens will provide holders with governance rights. See Aragon Network Whitepaper, Github (Aug. 28, 2018), https://github.com/aragon/whitepaper/blob/master/README.md [https://perma.cc/J72V-DY2V] (suggesting that token holders will be able to vote on issues like network upgrades, dispute resolution, monetary policy, and fiscal policy). Importantly, these governance features are only activated upon execution of a multisignature smart contract by holders instructed not to execute until the product launches. See Luis Cuende & Aragon, Introducing the Aragon Community Multisig, Aragon: Project Blog (May 15, 2017), https://blog.aragon.one/introducing-the-aragon-community-multisig-348a69d16374 [https://perma.cc/K8QM-63U2].

In our audit, we were unable to confirm that ANT tokens contain these latent governance rights. Rather, we discovered that governance features will be introduced through a future distribution of tokens which themselves will have the promised features.

186. Kik Interactive, Kin: A Decentralized Ecosystem, supra note 144, at 21.

187. Id. at 21–22.

188. Id. at 19.

189. See id. at 21. These tokens are allocated to fund the Kin Rewards Engine. See supra note 148 and accompanying text. Since the number of tokens being placed in circulation decreases over time, this feature also creates inflation for the token. Kik Interactive, Kin: A Decentralized Ecosystem, supra note 144, at 22.

190. Kik Interactive, Inc., Kin Rewards Engine 5 (2017), https://kinecosystem.org/static/files/Kin_Rewards_Engine_RFC.pdf [https://perma.cc/CNG9-TNCF] .

191. 4,601,252,295,287 Kin to be exact. Id. This is assuming a January 1, 2018, start date. Id.

FIGURE 10: KIN ALLOCATION CODE[192]

```
struct Grant {
    uint256 value;
    uint256 start;
    uint256 cliff;
    uint256 end;
    uint256 transferred;
    bool revokable;
}

function initTokenGrants() private onlyOwner {
    tokenGrantees.push(KIN_FOUNDATION_ADDRESS);
    tokenGrants[KIN_FOUNDATION_ADDRESS] =
        TokenGrant(MAX_TOKENS.mul(60).div(100), 0, 0, 3
        years, 1 days, 0);

    tokenGrantees.push(KIK_ADDRESS);
    tokenGrants[KIK_ADDRESS] =
        TokenGrant(MAX_TOKENS.mul(30).div(100), 0, 0, 120
        weeks, 12 weeks, 100);
}
```

This container variable is used to hold values pertaining to a specific grant.

This excerpt shows the hard-coded allocation of two grants—60% of the token supply to the Kin Foundation, and 30% to the Kik project.

The project implemented some of these promises in the code. The Kin smart contract creates vesting by maintaining a database of grants with a start date, end date, cliff, and installment length.[193] Grants are both creatable and revocable by the smart contract owner.[194] No more than 100 grants may ever be created and no address may receive a grant twice.[195] Every grant we have seen so far has a hardcoded cliff of one year, with two installments, one of which must be executed by the owner of the smart contract and on which is executed by the vesting trustee.[196]

When the Kin ICO commenced, the developers created two new grants. One corresponds to Kik's thirty percent stake and faithfully implements the ten percent per quarter vesting schedule described in the whitepaper.[197] Interestingly, the development team manually added a comment to the code showing that the address owning the stake belongs to Kik.[198] This suggests that Kik may have believed there would be at least some investor scrutiny over the technical governance features of its project.

The second grant corresponds to the sixty percent Foundation stake. We were unable to locate code for any of the highly detailed vesting mechanisms described in the whitepaper. We did observe that this grant is wholly controlled by the owner of a vesting trustee smart contract. Of course, offline ownership of that smart contract—the legal person within the Kin or Kik organization that actually receives the unlocked tokens—is

192. Kin (KIN), supra note 154.
193. See supra Figure 10.
194. See Kin (KIN), supra note 154.
195. See id.
196. See id.
197. See supra Figure 10.
198. See id.

not hardcoded into the Kin token code itself. It's simply bestowed on whoever has the private keys for that smart contract. In other words, there's nothing about the token code that enforces separate ownership of Kik's stake and the Foundation's. Instead, it depends entirely on the offline governance features of the project, enforced using traditional tools like corporate charters and bylaws (or not at all).

C. *Modifiability*

Beyond the specific protections against inflation of supply and desertion by key people, the promise of cryptoassets has also rested on the idea that investors are protected by the immutability of blockchain code. As we noted above, lawyers might well think of this as a wacky idea. And sure enough, immutability has indeed gone by the wayside for a number of ICO projects. Disclosure of what we refer to as "modifiability" is another matter. Though some token teams do advertise that tokens may provide new rights in the future, they do not explain that modification is a way to change any aspect of the token, not just activate valuable new features. And yet, as we will see, modification is built into the design of some ICO systems. How does this work?[199]

In the simplest setting, a developer can simply copy the contents of the data stored in a smart contract, and create a new smart contract, prepopulated with the data from the former. While those who owned tokens in the context of the original contract also own tokens in the new smart contract, the developer is free to create new code controlling the behavior of the latter. More concretely, an issuer may refuse to honor the original token when they finally complete development of the product the ICO was designed to fund.

This can be accomplished using two sets of rules: a primary smart contract with which users interact and a series of secondary smart contracts whose code is incorporated by reference.[200] Our lawyerly audience can think of the typical relationship between a website's Terms of Service and its Privacy Policy: The former usually contains a link to the latter, and purports to bind visitors to both.[201] Or, think of a public law that points to a private standard, like a city code that adopts LEED green-building

---

199. See infra notes 200, 204–215 and accompanying text.

200. See, e.g., Blackmoon Crypto Token (BMC), Contract Code, Etherscan, https://etherscan.io/address/0xdf6ef343350780bf8c3410bf062e0c015b1dd671#code [https://perma.cc/8CX2-QJ64] (last visited Feb. 16, 2019). A second approach to modification ensures the simultaneous removal of tokens from an existing contract and addition of equivalent tokens in a new contract. Users can upgrade to the new contract by manually calling a function in the old contract.

201. See, e.g., Woodrow Hartzog, Website Design as Contract, 60 Am. U. L. Rev. 1635, 1636 (2011) ("The social networking site [Facebook] has a Terms of Use Agreement with a section titled 'privacy.' The agreement references Facebook's privacy policy, a separate document.").

standards.[202] The standard can be updated privately, thereby modifying the effect of public law.[203]

A similar "pointing" mechanism enables the modification of cryptoasset smart contracts. All tokens using this method share identical code. The primary smart contract stores for each user the address of a secondary smart contract, containing the most recent set of accepted modifications.[204] The owner of the primary smart contract can modify the code by proposing a new secondary address, defining the smart contract whose terms will be incorporated. In one example we found (Monaco), the code gave users three days to opt in or out before the modification spread. When a user opts out, her current secondary smart contract address is frozen until the next time they explicitly opt in. The default state of all users is opt in, as illustrated below.[205]

FIGURE 11: MONACO MODIFICATION CODE[206]

```
function upgrade(uint256 value) public {
    balances[msg.sender] = safeSub(balances[msg.sender],
        value);

    totalSupply = safeSub(totalSupply, value);
    totalUpgraded = safeAdd(totalUpgraded, value);

    upgradeAgent.upgradeFrom(msg.sender, value);
    Upgrade(msg.sender, upgradeAgent, value);
}
```

202. See Sarah B. Schindler, Following Industry's LEED: Municipal Adoption of Private Green Building Standards, 62 Fla. L. Rev. 285, 289 (2010).

203. See id. at 303–07 (describing the process by which LEED certification standards are updated). This practice is, needless to say, controversial. See Nina Mendelson, Private Control over Access to the Law: The Perplexing Federal Regulatory Use of Private Standards, 112 Mich. L. Rev. 737, 748 (2014) ("[D]ecisions to incorporate private standards into the law . . . represent a potentially injurious public message that is inconsistent with core democratic values."); Schindler, supra note 202, at 316 (describing the advantages of standards developed in a public system, while recognizing the benefits private regulatory standards provide).

204. When a user executes a contract function, the primary contract checks the reference stored for the user and executes the incorporated code stored on the secondary contract.

205. Code for some tokens with modifiable contracts contained copyright notifications in the comments attributing the source to Ambisafe. See, e.g., Polybius (PLBT), Contract Code, Etherscan, https://etherscan.io/address/0x0affa06e7fbe5bc9a764c979aa66e8256a631f02#code [https://perma.cc/K66Y-9A26] (last visited Feb. 16, 2019).

206. This snippet illustrates the opt-in process in the Monaco contract. The user's account balance and total supply are decreased by the requested amount, the old contract runs a function on the new contract requesting that the tokens be "transferred," and finally, interested parties are notified via the "Upgrade" event. See Monaco (MCO), Contract Code, Etherscan, https://etherscan.io/address/0xb04cfa8a26d602fb50232cee0daf29060264e04b#code [https://perma.cc/FR29-3D54] (last visited Feb. 16, 2019).

The Polybius project provides another example. It is a proposed "fully digital bank accessible everywhere at any time . . . with a very efficient cost/revenue ratio."[207] Eventually, Polybius plans to "grow into your daily servicer and companion ecosystem . . . enabl[ing] secure and seamless connections between life and the things we love and use every day."[208] Investors contributing to the project can supposedly expect "higher returns" than those investing in traditional banks.[209]

The development team did make some limited claims about smart contract modification. The token purchase agreement explicitly states that "Polybius shall procure that the Smart Contract is modified and/or amended via an additional smart contract" to activate tokenholder voting.[210] It further specifies that the voting mechanism will enable the development team to propose changes to project smart contracts and to implement the changes if they receive two-thirds of tokenholder votes.[211] There are no further details.

However, we found modifiability functions in the smart contract code that extended well beyond changes to tokenholder voting rules, as Figure 12 details.

---

207. Polybius, Polybius Prospectus 1 [hereinafter Polybius Prospectus] (on file with the *Columbia Law Review*).

208. Id. at 2.

209. Id. at 1. The first step in this project was the sale of Polybius tokens (PLBT) to raise money for the Polybius Foundation. Id. at 3. PLBT gives holders rights more traditionally associated with stock or other forms of ownership. Id. It promises that holders will have the "right to receive a part of distributable profits of Polybius P.I. or Polybius Bank. All tokens in aggregate will have the right to receive 20% of such profits." Id. at 3. Note that this makes it highly likely that PLBT are securities. The prospectus recognizes as much, placing the following note at the bottom of each page:

> The tokens have not been and will not be registered under the United States Securities Act of 1933, as amended (the "Securities Act"), and may not be offered or sold in the United States or to or for the benefit of US persons (as defined in Regulation S under the Securities Act) unless they are so registered, or an exemption from the registration requirements of the Securities Act is available. One such exemption allows the resale of tokens purchased for their own account and for investment purposes only by investors who (i) are not otherwise affiliated with the Polybius Foundation, (ii) have been exposed for some time to the economic risks that ownership of tokens entails, and (iii) are not part of the distribution of the tokens.

Id. at 1.

210. Polybius Crowdfunding Terms & Conditions, Polybius, https://polybius.io/media/terms_and_conditions.pdf [https://perma.cc/K7XZ-Y5HM] [hereinafter Polybius Crowdfunding Terms & Conditions] (last visited Jan. 26, 2019).

211. See id.

FIGURE 12: POLYBIUS MODIFICATION CODE[212]

```
function getVersionFor(address _sender) constant
    returns(address) {
    return userOptOutVersion[_sender] == 0 ? latestVersion
        :
      userOptOutVersion[_sender];
}

function getLatestVersion() constant returns(address) {
    return latestVersion;
}

function optOut() returns(bool) {
    if (userOptOutVersion[msg.sender] != 0x0) {
        return false;
    }
    userOptOutVersion[msg.sender] = latestVersion;
    return true;
}

function commitUpgrade() returns(bool) {
    if (pendingVersion == 0x0) {
        return false;
    }
    if (pendingVersionTimestamp + UPGRADE_FREEZE_TIME >
        now) {
        return false;
    }

    latestVersion = pendingVersion;
    delete pendingVersion;
    delete pendingVersionTimestamp;
    return true;
}

function transferFromWithReference(address _from, address
    _to,
  uint _value, string _reference) returns(bool) {
    return _getAsset()
      ._performTransferFromWithReference(_from, _to,
          _value, _reference, msg.sender);
}
```

This function allows the contract to select the appropriate operative code for the user.

Here, the user can opt out of future contract updates.

The contract owner calls this function to confirm an update. This will succeed only if three days have passed since the modification was proposed.

This transfer code first obtains the code relevant to the current user using "getAsset."

Through this code, Polybius can propose modifications by deploying an entirely new secondary smart contract and linking it to the primary smart contract via the commitUpgrade function.[213] The primary smart contract does not allow the owner to make modifications directly—the owner must first propose the upgrade, which only takes effect after three

212. Polybius (PLBT), supra note 205.

213. See supra Figure 12.

days unless the user opts out.[214] In terms that legal readers will be familiar with, it is a "sticky default."[215]

Using these mechanisms, a development team can unilaterally change the tokens purchased by investors—or sometimes, propose changes that will be adopted if a certain percentage of users do not object.[216] Unless investors scrutinize both the potential for their tokens to be unilaterally modified, and the substantive terms of the modifications actually proposed, they are unlikely to discipline hasty or abusive changes. As we describe in Part IV, investors hardly pay attention to even simple nontechnical markers of quality. It is thus incredibly unlikely that they have the technical skills to monitor a development team's use of modification.

III. A SURVEY OF ICOS

Having identified three salient attributes of ICO governance, we now attempt to step back to look at a larger set of issuances to see how (and if) they dealt with governance issues. We reviewed the fifty largest 2017 ICOs by amount raised in dollars.[217] For each listed promotion, we scrutinized the whitepapers, token sale agreements, and computer code posted by the promoters. Appendix C pulls quotes about supply, burning, vesting, and modification (if they are available) from the issuers' public statements.[218] We compared those promises, read by investors, with what we discerned from close examination of software code. Our approach is empirical, but obviously neither comprehensive nor representative of all 2017 ICOs.

---

214. See supra Figure 12.

215. For the classic initial treatment, see generally Omri Ben-Shahar & John E. Pottow, On the Stickiness of Default Rules, 33 Fla. St. U. L. Rev. 651 (2006).

216. It is similar to a reverse collective action clause. See generally W. Mark C. Weidemaier & Mitu Gulati, A People's History of Collective Action Clauses, 52 Va. J. Int'l L. 51, 52–55 (2013).

217. As discussed in section IV.B below, there are major challenges involved in sourcing even the most basic information about this market. Finding a list of the largest ICOs is one such example. The amount of funds raised in ICOs are self-reported and listing sites rarely scrutinize their own figures. Further, there are omissions of important ICOs and other discrepancies across the various listing sites. We essentially used a list of the top fifty 2017 ICOs compiled by Coinschedule, with three notable exceptions. The site omits the Grid+ ICO, which raised about $38.5 million in its presale and ICO, as well as Tron, a controversial project that raised $70 million in its presale and ICO. See infra Figure 13 (summarizing ICOs and amounts raised). These projects would both be within the top thirty of our sample, so we manually added them to our list. Additionally, we omitted one project that was listed by Coinschedule. Sonm, which apparently raised $42 million, does not have an accessible original whitepaper. This made it impossible to determine its claims about token functionality.

218. See generally Appendix C, supra note 69.

A. *The Scene from 50,000 Feet*

The fifty firms we studied were reported to have raised a total of approximately $2.6 billion at their ICOs and the notional initial market cap was $7.0 billion.[219] In the sample, nineteen were headquartered in the United States, six in Singapore, and the remaining in a variety of countries, including Switzerland (five), England (two), China (two), Estonia (two), and Thailand (two).[220] By January 2019, eleven of the projects had not released any kind of alpha version or demo of their project.[221]

Our approach to auditing is limited: We try to take the position of a sophisticated, but time-constrained, investor. Consider, again, Polybius. Its whitepaper makes several claims that would lead us to expect certain features directly coded into tokens or other smart contracts. The most striking example is the team's promise that "according to the conditions of the ICO, payouts to tokenholders are directly connected to the earnings of the Polybius project."[222] The team goes on to specify a range of offline activities that will support payment of the dividend, like preparation of audited financial statements, and tells readers to expect dividend payments in Ethereum.[223]

Beyond ERC-20 compliance and the presence of a modification feature, we did not verify that any of these features are present, largely because Polybius's coded governance exists in bytecode (which, as you will recall, is the Ethereum machine language). Without spending a large sum of money purchasing the time and know-how of a very motivated and talented reverse engineer, an investor would have to rely

---

219. See infra Appendix A.

220. See infra Appendix A.

221. See infra Appendix A.

222. satoshi092, What Are Polybius Tokens and Why Should They Be in Every Crypto-Investor's Portfolio?, Steemit (Aug. 9, 2017) https://steemit.com/cryptocurrency/@satoshi092/what-are-polybius-tokens-and-why-should-they-be-in-every-crypto-investor-s-portfolio [https://perma.cc/4XBK-2CPJ]; see also Polybius Prospectus, supra note 207, at 6 (noting that moneys raised will be used "mainly, but not exclusively on acquisition of licenses, building out the systems, hiring the team and marketing").

223. See Polybius, Polybius Token Whitepaper 4 (2017), https://polybius.io/media/token_whitepaper.pdf [https://perma.cc/VV8L-VBXE]; see also Polybius Crowdfunding Terms & Conditions, supra note 210 ("'Smart Contract' means the Ethereum smart contract made for Polybius . . . and is the mechanism of the distribution of Payouts to the Token holders as described in the Token Whitepaper."). There was ample mention of dividends in the terms and conditions that governed token purchases, which calls the dividends "Payouts." Polybius Crowdfunding Terms & Conditions, supra note 210. That old-fashioned contract specifies that token holders are "eligible for obtaining Payouts according to their stakes" and that the token code is "the mechanism of the distribution of Payouts." Id. It even provides ways to adjust the Payout calculation in the event that Polybius repurchases and burns some circulating tokens, or to account for dilution if Polybius receives new equity financing. Id.

on vernacular promises.[224] Below is an excerpt of what the public-facing code (incorporated by reference) looks like.

FIGURE 13: POLYBIUS BYTECODE[225]

```
0x6060604052361561 00f65763ffffffff60e060020a6000350416
631962df7181146100fb57806319ab453c1461017a5780631a1fea
e1146101a757806321538acb146101c657806324c65f35146101e5
5780633f2f1596146102045780634f6d3aed14610234578063 5b36
fea6146102535780636361d027b3146102725780637a386e88146102
9b5780637afa8388146102c8578063a39385de146102e7578063a4
b7459a14610306578063c10796df14610325578063c358d4ff1461
039b578063cca97025146103cb578063db00b84814610452578063
e34f7137146104bd578063eb58705b146104f4578063ec55688914
610575575b610000565b346100005760408051602060046435 81
```

This shows that it is not merely the case that the investment depends on the development team's decision to actually build the products it hypes in its whitepaper.[226] Investors must also have faith—either that ordinary contract law litigation will back up old-fashioned terms of use, or that the bytecode, which essentially no one can or will parse, renders those promises operable.

Putting unauditable smart contracts to one side, here are the results of our analysis, which compares the software to promises made in whitepapers, blog posts, and websites marketed to investors.

B. *Supply Promises: Scarcity and Burning*

We begin with promises regarding supply. Of the fifty tokens, we audited the code of forty-five (four remain in bytecode or in proxy contracts, and one, FileCoin, has not released any code or token). We dropped projects without auditable code from our analysis. Figure 14 illustrates how such firms approached supply scarcity commitments.

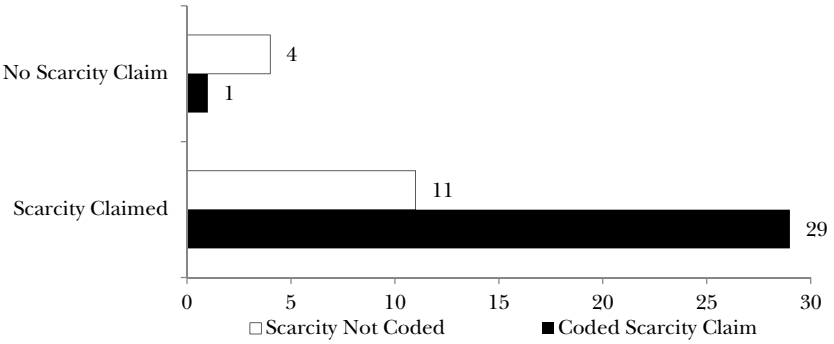
---

224. Analyzing bytecode involves tracing both the low-level flows of data and arithmetic in order to reconstruct a contract's logic. It requires meticulous attention to each individual machine operation, and a memory to retain the state of the virtual machine at each step. For an introduction to bytecode, see Bernard Peh, Solidity Bytecode and Opcode Basics, Medium (Sept. 17, 2017), https://medium.com/@blockchain101/solidity-bytecode-and-opcode-basics-672e9b1a88c2 [https://perma.cc/Q4PE-DYBM].

225. The main contract incorporates by reference code to perform most tasks. The figure shows an excerpt of the bytecode referenced. While a skilled analyst can reconstruct the function of the code, such analysis is beyond our scope. See Polybius (PLBT), supra note 205.

226. Note that the Polybius team actually decided to release a different project than the one described in the whitepaper. Tzao Se, Past ICO Review: Why You Can't Take Polybius to the Bank, U.Today (July 23, 2018), https://cryptocomes.com/past-ico-review-why-you-cant-take-polybius-to-the-bank [https://perma.cc/BWP8-L8JQ]. The team claimed that this was due to an E.U. regulation that was released years before the ICO. Id. This underscores the point that after an ICO, a development team is able to do whatever it wants with the funds raised.

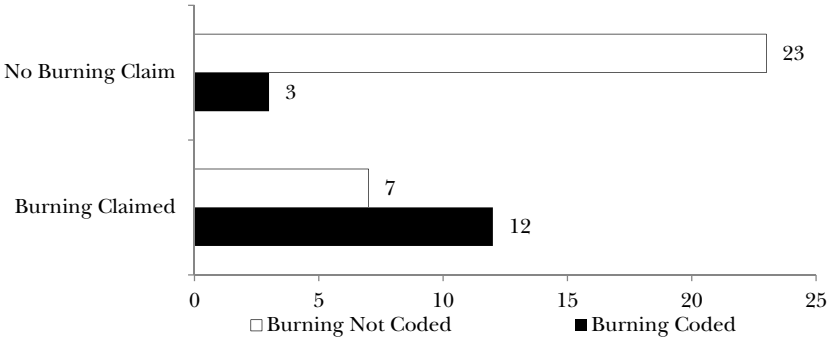
FIGURE 14: SCARCITY AUDIT RESULTS[227]



Almost all issuers promise a supply restriction in their marketing documents (40 of 45, or approximately 90%). And most of those that promise a restriction deliver it (29 of 40, or approximately 75%). Overall, though, only about two in three (29 of 45, or approximately 64%) firms that we audited encoded a supply restriction. To be clear, this is not to say that the firms that did not deliver coded scarcity limits actually promised to do so—their marketing promises either did not mention scarcity or may not have discussed how it was to be effected.

The second sort of supply promise—burning—displays a different pattern. Figure 15 details our burning audit.

FIGURE 15: BURNING AUDIT RESULTS[228]



Here, fewer firms promised to burn tokens than promised to cap supply in the initial mint (19 as compared to 40). Of those that promised to burn supply, approximately 36% (7 of 19) did not fix that claim with code.

227. See infra Appendix B. "Scarcity Claimed" in the Figure is a designation for those issuers that promised a supply restriction in their marketing documents.

228. See infra Appendix B.

C. *Vesting Promises*

Of the forty-five auditable issuers, thirty-six promised vesting in their marketing documents or whitepapers, while nine did not. Figure 16 illustrates our findings.

FIGURE 16: VESTING AUDIT RESULTS[229]

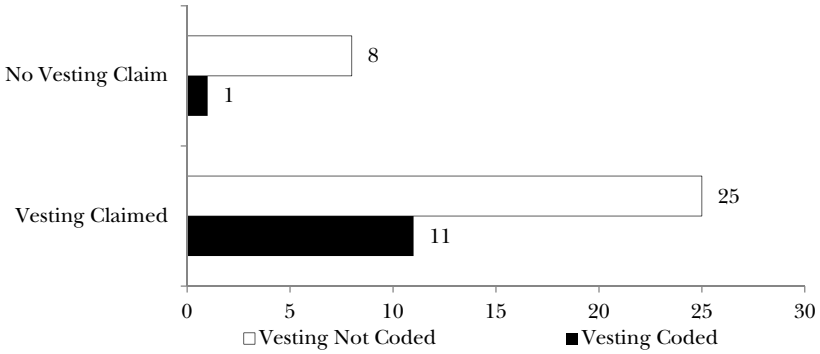


Figure 16 illustrates first that almost 20% of the sample did not promise to vest at all, which is a surprising result given the amounts raised. Second, of the 80% that promised to vest, the vast majority apparently did not use smart contracts to encode those rights.[230]

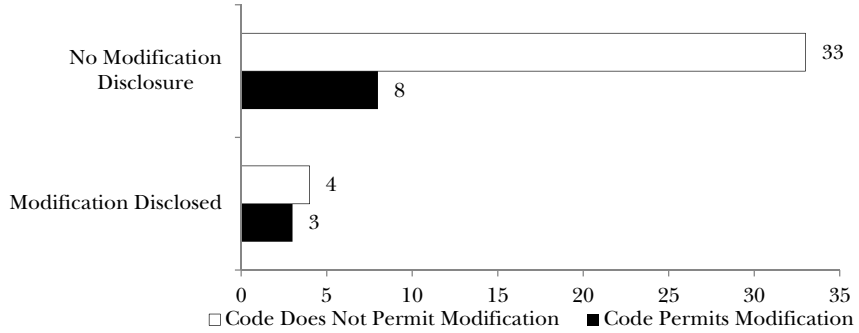
D. Modification Promises

Finally, we describe the modification rules in the sample. Modification is rarely discussed in marketing materials: Only seven of the fifty firms discussed the token's modifiability in their marketing materials or soft contracts. But overall, twelve of the fifty firms permit modification through their code. While most (4 of 7) of the firms that disclosed modification had code that backed up their promises, eight firms that did not discuss modification permitted it.

229. See infra Appendix B.

230. Some projects use secondary smart contracts to encode vesting, such as the Basic Attention Token. So long as the tokens transferred before the ICO, we would count that as a coded vesting. According to Brendan Eich, BAT used this two-stage structure to have "simple, do-as-few-things-as-possible smart contracts. We were keenly aware of all the problems other projects to that date . . . had trying to get fancy with Solidity." Email from Brendan Eich to David Hoffman (July 30, 2018) (on file with the *Columbia Law Review*).

FIGURE 17: MODIFICATION AUDIT RESULTS[231]



E. *Summary*

To sum up: There are significant differences between code and contract in our sample.[232] Projects are making governance claims that look to be modeled off of offline VC or traditional equity-based rules intended to reduce agency costs, but they are not encoding those promises into the sort of trustless, decentralized systems which undergird their networks' purported sky-high values.

IV. COIN-OPERATED CAPITALISM?

So far, our inquiry has been motivated by two goals. First, we have tried to capture the reality of the ICO form as it existed in 2017–2018—a snapshot of a supposedly revolutionary innovation just after its birth. Second, we have attempted to understand smart contracts at a deep level of contextual detail. They are at the heart of the innovation story told by ICO proponents, some of whom claim that code will increasingly be able to replace traditional law.[233] We have traced their early history,[234] explained how they were expected to function in the ICO market of 2017,[235] and taken stock of the reality.[236] In this Part, we evaluate the distance between expectations and reality.

As we established in Part III (and in detail in Appendix B), for over 20% of ICOs in our sample where promoters promised cryptoasset supply restrictions, and 35% of promised token burning, we could not observe

231. See infra Appendix B.

232. For the results in summary form, see generally infra Appendix B.

233. See De Filippi & Wright, supra note 24, at 102–03 ("Token sales are the Wild West of financing, and by using blockchain technologies and decentralized exchanges, companies, projects, or organizations can continue to raise funds by relying on lex cryptographica, ignoring geographic rules and regulations governing public markets and securities trading.").

234. See supra Part I.

235. See supra Part II.

236. See supra Part III.

restrictions hard-coded into smart contracts. More starkly, we could not find hard-coded vesting restrictions in twenty-five of the thirty-six ICOs where promoters promised to adhere to such restrictions. Finally, of twelve ICOs for which our audit revealed that a central party could modify the functionality of the cryptoasset's smart contract code, only four disclosed that ability in their promotional materials.

Our results raise serious questions about the role of code in ICOs. Do investors punish ICOs that fail to build key protections into code or fail to disclose the power of modification? If not, is that because code does not matter as much as its proponents claim it does? Or is it because the ICO market is broken? We examine those questions in the sections that follow.

A. *Paper, Code, and Market Response*

For a minute, let's look at our results from the perspective of an ICO advocate who believes that code has the potential to be a cheaper and better way of delivering investor protections than traditional venture financing routes. Should this person be troubled by our results? At one level, the answer has to be yes. The fact that a majority of the leading ICOs—each of which raised over $20 million—fail to write their own vesting promises into code is inconsistent with a story about code replacing law. It also raises serious questions about whether investors are adequately protected from founder desertion.

But our ICO advocate might push back. Perhaps we are wrong about the absence of hard-coded rules (and if we are, we hope to be corrected). Or, maybe, investors do take the problems we observed in Part III into account when investing. That is, maybe problems with coded investor protection are reflected in market prices.

Though the ICO market is young, we are skeptical of this "investor-protection code is priced" thesis. As a first cut, the sheer number of problems in our sample suggests otherwise. Our results show that the majority of the top-grossing ICOs of 2017 had major problems with how code bore out their antiexploitation disclosures.[237] To quantify the idea of paper–code distance, we refer to any uncoded investor protection for supply, burning, vesting, or incongruence between code and disclosures regarding modifiability as "distance." Using these data, we score each ICO from zero to four.[238] Of the fifty ICOs, we give forty-nine a score because we can evaluate either the token or the associated smart contracts. Fourteen have no distance, nineteen have one marker, twelve have two, three have three, and one (Monaco) has four. If investors know

---

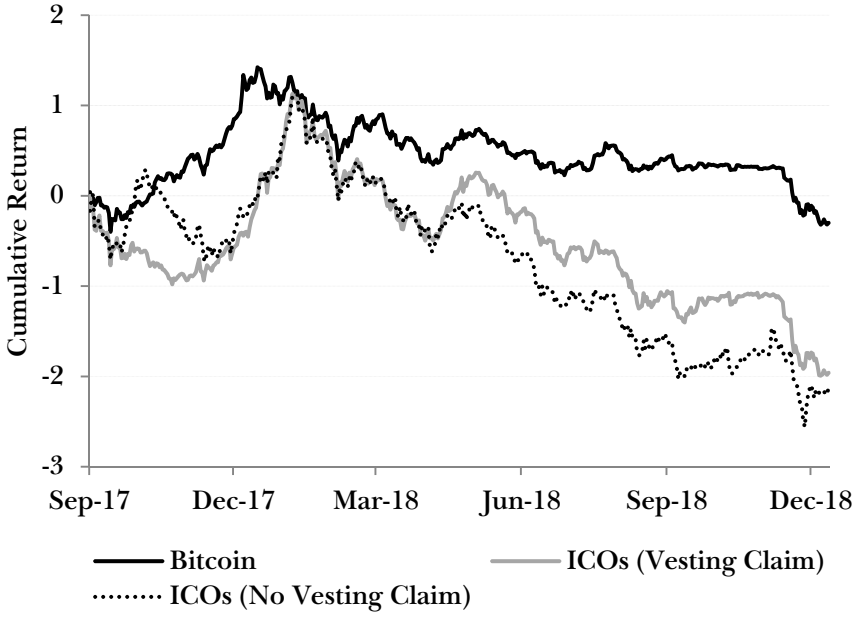
237. See infra Appendix B.

238. That is, the token gets a 1 for scarcity claims not matching code, a 1 for vesting claims not matching code, a 1 for burning claims not matching code, and a 1 if it has undisclosed modification terms.

about the problems we've identified, then the makeup of the top fifty suggests that they don't much care.

Nor do the postsale market metrics we are able to observe enable us to say a great deal about the "code is priced" thesis. We do not see significant changes in code congruence over time, and we lack a natural experiment on initial code pricing. What we can observe is whether (over time) firms that encode their disclosures have different returns and trading volumes. An approach suggested to us by a commentator on an earlier draft of this paper[239] was to develop a rolling weighted portfolio of the prices (and trading volume) of our fifty projects, controlling for their disclosed and coded governance rules. Using this approach, we find that—consistent with earlier work—disclosed governance rights do seem to promote better returns.[240]

FIGURE 18: VESTING DISCLOSURES AND ROLLING AVERAGE CUMULATIVE RETURNS[241]



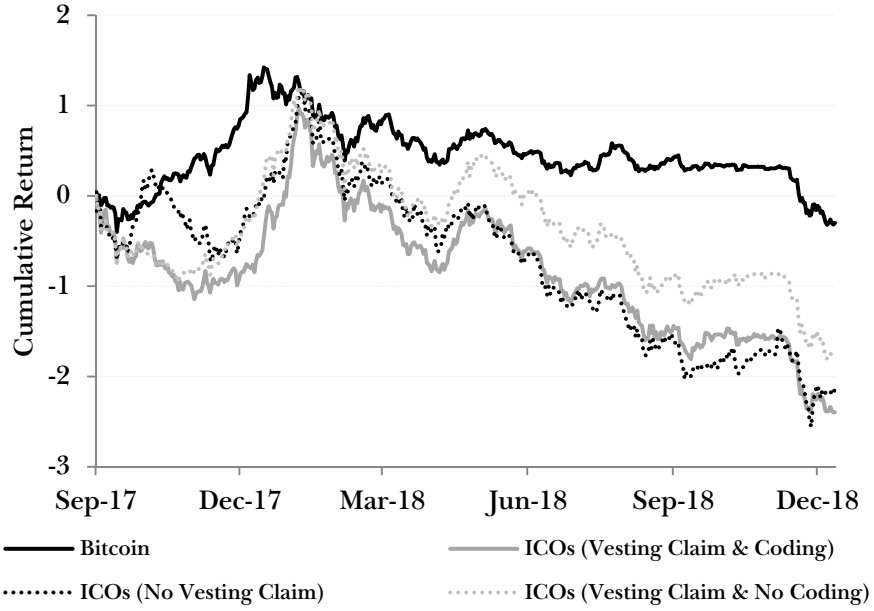
239. We thank Professor Robert Bartlett for his suggestion and the data that gave it life.

240. See supra note 31.

241. Data from CoinMarketCap, courtesy of Professor Bartlett. Bartlett pulled daily volume and price data from coinmarketcap.com and created a weighted average portfolio using our coding about project quality. We modified his work when later checking revealed minor changes in the coding of particular projects. Both the .do and the underlying data are on file with the authors and the *Columbia Law Review*.

The next figure repeats the first, but now breaking out projects that coded vesting and those that promised but did not code it.

FIGURE 19: VESTING (CODED VS. DISCLOSED) AND CUMULATIVE RETURNS[242]



Here, we can see that firms that coded vesting had returns that were indistinguishable from those that did not code it. Professor Robert Bartlett reported similar results on scarcity, as well as trading volume. In a series of regressions, he found while disclosure of vesting and scarcity were correlated with higher returns, coding of those attributes had no consistent and significant effects.[243] Trading volume and price were, however, closely tied to Bitcoin's price and trading volume, a result that fits with other recent research.[244]

Finally, we are skeptical of the "investor-protection code is priced" thesis because buy-side literature in 2016–2018 rarely treated the guts of code as something worth considering. Like stocks, ICOs have developed a wide range of secondary information sources, including "ratings" websites. But most of these raters do not vet smart contract code. Of the

242. For information regarding from where this data set was obtained and the procedures performed on it, see supra note 241.

243. The authors' regression files are on file with the *Columbia Law Review*.

244. See Griffin & Shams, supra note 8, at 33 (indicating that Tether, a digital currency, influences Bitcoin pricing).

top five English-language rating sites by Alexa ranking, which measures how popular a website is,[245] only one posts information about code quality, though not of significant detail.[246] Similarly, code takes a backseat to other investment drivers in the retail valuation literature.

In the period before 2017, advisory publications focused on a project's ability to deliver anonymity and decentralized governance, which in turn was thought to help hedge against regulation.[247] In the period after 2017, guides focused on the potential for widespread functional use within the startup's system,[248] the reputation and involvement of the founders and creative team,[249] and the avoidance of obvious scams.[250]

---

245. Kim Kosaka, What Is Alexa Rank?, Alexa Blog, https://blog.alexa.com/marketing-research/alexa-rank/ [https://perma.cc/MQP5-68UV] (last visited Mar. 19, 2019).

246. We use ICOnow to identify the top five ratings sites. Top ICO Listing Sites, ICOnow, http://iconow.net/all-ico-calendarlisting-sites-with-alexa-rank-and-traffic/ [https://perma.cc/WQ8K-8LVP] (last visited Jan. 27, 2019). Four of these sites do not analyze smart contract code: (1) icodrops.com (Alexa rank: 14,206); (2) icobench.com (Alexa rank: 15,078); (3) coinschedule.com (Alexa rank: 18,861); and (4) cryptopotato.com (Alexa rank: 136,699). Id. Only one of the four sites does analyze smart contract code: icorating.com (Alexa rank: 79,549). Id. However, the site's attention to code is thin. While it mentions smart contracts on its "methodology" page, it does not regularly (if ever) analyze any code itself. See Project Evaluation, ICORating, https://icorating.com/methodology/ [https://perma.cc/WXS6-UGH6] (last visited Feb. 17, 2019).

247. See, e.g., Roger Aitken, German Blockchain Startup BlockPay "Bootstrapped" with Crypto ICO Investment, Forbes (Aug. 20, 2016), https://www.forbes.com/sites/rogeraitken/2016/08/20/german-blockchain-startup-blockpay-bootstrapped-with-crypto-ico-investment/ [https://perma.cc/3A65-GE8G] ("For criminals and legitimate businesses alike, the blockchain's transparency could pose a real problem. . . . If you can figure out where the money is going, you can gain a major competitive edge over a company."); Marco Santori, Appcoin Law: ICOs The Right Way, CoinDesk (Oct. 15, 2016), https://www.coindesk.com/appcoin-law-part-1-icos-the-right-way/ [https://perma.cc/2BDP-FEHR] ("Appcoin developers should consider building products . . . which run . . . in a decentralized fashion. The more unaffiliated developers contributing to the development and operation of the product, the less likely any profit . . . is to be considered 'from the efforts of others'—and the less likely vertical commonality will be present.").

248. See, e.g., Chinedu Adeyemi, Cryptocurrency: How to Start? Guide to Cryptocurrency Trading for Beginners, The Oofy (June 2, 2018), https://theoofy.com/13199/cryptocurrency-how-to-start-guide-to-cryptocurrency-trading-for-beginners/ [https://perma.cc/Y7XW-FNT9] ("Some coins seem to keep increasing in value simply due to supply-demand factors. This trend might not be sustainable. For a coin to have [long-term] supported value, it must have a real-world use case eventually.").

249. How to Choose an ICO to Invest In, Cointelegraph, https://cointelegraph.com/ico-101/how-to-choose-an-ico-to-invest-in#read-the-white-paper [https://perma.cc/UPZ3-Q3LK] (last visited Jan. 27, 2019) (advocating for potential investors to "[f]ind out everything [they] can about the development team" and to "make sure that the developers are not anonymous").

250. See, e.g., John Wasik, Why Millennials Are at High Risk for Bitcoin & ICO Fraud, Forbes (Mar. 5, 2018), https://www.forbes.com/sites/johnwasik/2018/03/05/why-millennials-are-at-high-risk-for-bitcoin-ico-fraud/ [https://perma.cc/MYB2-NU5L] ("One simple way to avoid fraud is to reject solicitations. Whenever you see a mobile ad or email telling you about overnight riches in cryptocurrencies, avoid clicking on their links.").

Eventually, some investors gave up on ICOs completely.[251] But there's never been an emphasis on checking that coded governance actually happens.

For instance, while the bestselling *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond* does exhort investors to scrutinize developer activity,[252] it does not view the actual product of developer activity—the code—on the same plane. Indeed, the book does not include a project's codebase in the materials that it suggests a fundamental-analysis investor would want to consider.[253] To the authors of most buy-side advice, cryptocurrency investment is an exercise in reading whitepapers, blog posts, and commentary—and watching the social-media trade winds—but rarely involves inquiry into code.[254] Taken together with analysis of our sample, these impressionistic sources of evidence lead us to believe that investor-protection code is not a significant driver of market pricing.[255]

ICO advocates might reasonably respond to this absence of evidence for the importance of code in a number of ways. First, it might be the case that investor-protection code will manifest itself as a driver of market returns in the future. Perhaps future researchers will develop measures that capture price tremors in response to phenomena like the one we identified in Part III. It is also possible that the ICO market's "crypto winter" was driven by investors who scrutinized the code of circulating tokens and found it lacking.

Some commentators do advise investors to pay attention to the underlying code of cryptocurrency projects, and their approach may be gaining adherents.[256] Further, some ICO promoters take to Reddit

---

251. See supra note 19.

252. See generally Burniske & Tatar, supra note 31.

253. See id. at 172–73 (discussing the materials necessary to conduct fundamental analysis of cryptoasset investments).

254. See, e.g., Reza Jafery, Cryptocurrency Fundamental Analysis: 4 Ways to Gauge the Strength of a Community, Hacker Noon (Jan. 8, 2018), https://hackernoon.com/4-ways-to-gauge-the-strength-of-a-cryptocurrencys-community-4b42c0e5d735 [https://perma.cc/U6QJ-HBQV]; Simon Kertonegoro, Fundamental Analysis: How to Judge a Cryptocurrency's Intrinsic Value, Medium (Mar. 12, 2017), https://medium.com/@esscay/fundamental-analysis-how-to-judge-a-cryptocurrencys-intrinsic-value-a3d789da94e1 [https://perma.cc/HNA3-L3LE]; Dean Patrick, On Tokenomics and ICO Valuations, Medium (Jan. 13, 2018), https://medium.com/@deanpatrick_63570/on-tokenomics-and-ico-valuations-5312e5bdc2bd [https://perma.cc/V8UH-DNXW].

255. Aside from Rhue, supra note 31, at 20, who finds that identification of "bugs" on Etherscan is associated with lower market capitalization, we are aware of no other analysis of the relationship between code and market value.

256. See Rohr & Wright, supra note 18, at 27 n.73 (suggesting that failure to list code in an open source site "may signal ulterior motives on the part of the party selling the token"). Others agree. See How to Choose an ICO to Invest In, supra note 249 ("Evaluate the quality of the code. If a project has no working code whatsoever prior to an ICO, or even if they do, but it isn't open source—that's a major red flag."); Michiel Mulders, 10 Keys for Evaluating Initial Coin Offering (ICO) Investments, CryptoPotato (Apr. 26, 2018), https://cryptopotato.com/10-keys-evaluating-initial-coin-offering-ico-investments/ [https://

message boards to offer bounties to independent parties interested in auditing smart contract code—an indication that attention to code (or at least the perception of attention to code) is valuable from the promoter perspective.[257] These audits focus on the antihacking aspects of cybersecurity, not specific instantiation of economically relevant promises.[258] But perhaps the recent "modifiability crisis" after the Bancor hack will bring our investor-protection concepts to the fore. In other words, the market will reflect investor protections found in code sooner or later.[259]

A second potential response from our ICO advocate might take a different tack. Instead of defending the importance of code in delivering investor protections, the advocate might retreat and take up a holistic defense. Specifically, even if code is failing to protect investors, there still

---

perma.cc/9NZ3-HF55] ("The quality of a developer can be understood by analyzing some of their code . . . . Avoid messy developers.").

257. A search of "ICO audit" of the Etherium Community's Developer Reddit evidences as much. See, e.g., bfjs123, Best Way to Get My ICO Contract Audited?, r/ethdev, Reddit (Feb. 6, 2018), https://old.reddit.com/r/ethdev/comments/7vq3s0/best_way_to_get_my_ico_contract_audited/ [https://perma.cc/8DVU-AR7R]; Bspendcom, Looking for ICO Security Audit, r/ethdev, Reddit (Oct. 12, 2017), https://old.reddit.com/r/ethdev/comments/75wz6m/looking_for_ico_security_audit/ [https://perma.cc/TA54-Y9SC]; Cointed, [BUG BOUNTY][ICO] Cointed Token Audit (100k EUR Reward!), r/ethdev, Reddit (Oct. 12, 2017), https://old.reddit.com/r/ethdev/comments/75x5kb/bug_bountyico_cointed_token_audit_100k_reward/ [https://perma.cc/4AMQ-TJZP].

258. See, e.g., Cimpanu, supra note 114 (citing industry study). This auditing is quite important, of course. See Anna Irrera, More Than 10 Percent of $3.7 Billion Raised in ICOs Has Been Stolen: Ernst & Young, Reuters (Jan. 22, 2018), https://www.reuters.com/article/us-ico-ernst-young/more-than-10-percent-of-3-7-billion-raised-in-icos-has-been-stolen-ernst-young-idUSKBN1FB1MZ [https://perma.cc/PS5P-63XZ] [hereinafter Irrera, More Than 10 Percent]. ICOcheck.io does feature crowdsourced evaluations of the presence or absence of smart contract provisions, including hard-coded vesting constraints. See ICO Checker, icochecker.com, [https://perma.cc/H3QX-EYJP] (last visited Jan. 26, 2019). But its Alexa rank is in the millions, in contrast with the top five sites, which range in ranking from 136,699 to 14,206. See supra note 246.

259. Much of the excitement over ICOs has shifted to a new form of token-based fundraising: the "security token" offering, or STO. STOs are ICOs in which issuers embrace the security-like nature of their tokens, adhering to SEC rules governing offers and sales, while adding features of traditional instruments like cash flow or governance rights. The imminent rise of STOs could give the SEC a greater opportunity to address consumer protection risks posed by token sales. Or, enthusiasm for STOs could be pure hype. See, e.g. Aashish Sharma, Will STOs (Security Token Offerings) Rule Over ICOs in 2019?, Hacker Noon (Jan. 12, 2019), https://hackernoon.com/will-stos-security-token-offerings-rule-over-icos-in-2019-8feda7bcf562 [https://perma.cc/89EP-RBSA] ("We have it on a good source that the estimated growth of STO is . . . $10 trillion over the next few years."); Syed Shoeb, Will 2019 Be the Year of the STO?, Hacker Noon (Dec. 17, 2018), https://hackernoon.com/will-2019-be-the-year-of-the-sto-understanding-stos-security-tokens-market-potential-over-icos-4d2502227220 [https://perma.cc/3L5E-FT38] (explaining that STOs are ICOs with "certain regulations that hold the token issuers accountable"). For an overview on the technical tradeoffs involved in STO issuance, see Matthew Finestone, The 2019 Truth on Security Tokens, Loopring Protocol (Dec. 21, 2018), https://medium.com/loopring-protocol/the-2019-truth-on-security-tokens-7800c14129e4 [https://perma.cc/28WM-AP5U].

remain legal and reputational checks on exploitation and desertion by ICO teams. That is, there will be *substitutes* for coded governance rules. Instead of the law of the blockchain, the law of the Swiss *stiftung*, the California Business Practices Code, and the Securities Act of 1933 will ensure that bad actors are punished, and the market will do the rest.[260]

As we argued above, the legal safeguards against ICO investor exploitation are, at present, significantly weaker than in other investment markets.[261] It is easy for an issuer to set up shop in a low-regulation jurisdiction,[262] and the architecture of the cryptoeconomy enables far more user and promoter anonymity than typical markets.[263] And even for transparent issuances conducted in the shadow of U.S. law, our background legal regime presents untested forms of investor protection. While a number of class-action suits, largely premised on state law violations, have been filed against some prominent ICO teams, the viability of any of their claims remains unclear.[264] The deterrent threat of legal ramifications is not nearly as strong as in typical markets—and, of course, is far weaker than the automated enforcement of code.

At a deeper level, arguments about the power of traditional legal deterrence are dangerous for ICO advocates. They show that advocates have already abandoned the high ground of "lex cryptographica."[265] Smart contract code was, after all, supposed to render traditional intermediaries useless, obviate the need for regulation, and reduce transaction costs for participants.[266] Without those justifications, it becomes harder to see what benefits ICOs provide, other than regulatory arbitrage.

To be explicit, if the value of blockchain-based financial products turns on the reputations of their creators or the vitality of legally enforceable wrap contracts, we see no good reason why traditional regulatory tools—

---

260. These are some of the bodies of paper law that plaintiffs have invoked in their lawsuits against Tezos and Paragon, for instance. See Complaint at 2, Davy v. Paragon Coin, Inc., No. 18-cv-00671 (N.D. Cal. Jan. 30, 2018), 2018 WL 653425; Complaint at 19, Gaviria v. Dynamic Ledger Sols., Inc., No. 6:17-cv-01959 (M.D. Fla. Nov. 13, 2017), 2017 WL 5713392; Complaint at 5, Baker v. Dynamic Ledger Sols., Inc., No. CGC-17-562144 (N.D. Cal. Oct. 25, 2017), 2017 WL 5022656.

261. See supra Part II.

262. See Rohr & Wright, supra note 18, at 30–31, 96.

263. See, e.g., Shifflett & Jones, supra note 8; John O. McGinnis & Kyle Roche, Bitcoin: Order Without Law in the Digital Age 30–33 (Nw. Pub. Law Research Paper No. 17-06, 2018), https://ssrn.com/abstract=2929133 (on file with the *Columbia Law Review*); Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli & Roberto Saia, Dissecting Ponzi Schemes on Ethereum: Identification, Analysis, and Impact 1 (Mar. 10, 2017) (unpublished manuscript) (on file with the *Columbia Law Review*).

264. See supra note 260 and accompanying text.

265. Cf. De Filippi & Wright, supra note 24, at 193–204 (arguing that ICOs can rely on "lex cryptographica" to enforce investor protections).

266. See, e.g., ChainTrade, 10 Advantages of Using Smart Contracts, Medium (Dec. 26, 2017), https://medium.com/@ChainTrade/10-advantages-of-using-smart-contracts-bc29c508691a [https://perma.cc/65H6-87GT] (describing in greater detail these classic arguments raised in support of smart contracts).

securities law, know-your-customer regulations, and fiduciary suits—should not heavily police a space that currently is rife with the opportunity to bilk investors. The analogy to the failures of the pre-1933 securities regime would be unavoidable.[267]

However, we are not ready to make that sort of strong claim about the missing role of intermediaries. Some projects encode all of their governance protections, and others appear to fall short largely only on vesting.[268] We simply do not know enough at the moment about what incentives encouraged particular turns to coded governance. Nor have we investigated the more mature 2018 market. Today, several sites are working to develop informally rich certification systems.[269] Perhaps such systems will evolve and further depress the need for old-fashioned intermediation in the absence of regulation.

But perhaps not. If problems with investor protection code are not priced into the market, and traditional law presently has trouble deterring abuses, where does that leave us?

B. *Whose Market Is This?*

The absence of evidence suggesting that investors are well-protected in the ICO market raises a natural question for legally-minded readers: Should we regulate this thing? Some see evidence of fraud and call for the whole market to be shut down.[270] Others would like the state to keep out.[271] Each approach has costs and benefits, of course—a conundrum where good things like innovation, investor protection, and regulatory clarity sit uneasily alongside each other.[272] There are tradeoffs galore.

For the pragmatists out there, a lot depends on who is being protected, and who benefits from innovative change. Are the investors actually

---

267. See Carol J. Simon, The Effect of the 1933 Securities Act on Investor Information and the Performance of New Issues, 79 Am. Econ. Rev. 295, 296–97 (1989) (describing briefly the failures in the market that led to the passage of the Securities Act of 1933).

268. See supra Part III.

269. See, e.g., Messari Disclosures Registry, Messari, http://messari.io/registry (on file with the *Columbia Law Review*) (last visited Jan. 27, 2019).

270. This has been the approach taken, for example, by regulators in China and South Korea. See Zetzsche et al., supra note 16, at 30–32.

271. See, e.g., Richard Waters, To Coin a Craze: Silicon Valley's Cryptocurrency Boom, Fin. Times (Sept. 13, 2017), https://www.ft.com/content/2b0d8926-96d9-11e7-b83c-9588e51488a0 (on file with the *Columbia Law Review*) (quoting Tim Draper as stating that "ICOs are filling in where governments have failed"); cf. Max Raskin, The Law and Legality of Smart Contracts, 1 Geo. L. & Tech. Rev. 305, 333–40 (2017) (arguing for a light hand on smart contract regulation).

272. See generally Chris Brummer & Yesha Yadav, Fintech and the Innovation Trilemma, 107 Geo. L.J. 235 (2019) (describing a theoretical framework for understanding the competing goals of clarity, innovation, and market integrity that regulators seek to balance when confronting new financial technology).

grandparents risking their retirement savings?[273] Or are they day-traders enjoying a virtual casino?[274] We might want—really, we do want—to protect mistaken elders more than thrill-seekers.[275] We also must be aware that regulations often will protect first-movers against competition by setting up new barriers to entry. And any serious regulatory strategy needs to help combat cryptoassets' role in supporting illicit markets.[276] To inform the best approach to regulation, we need to know a lot more about the ICO buy side.

We see four archetypal participants on the buy side in the ICO market. Each has different implications for how to interpret the sell-side picture we have painted in this Article. Gaining a better read on the precise ratios and combinations of each will be a key next step for scholars and policymakers who deal with ICOs.

1. *Irrational Exuberance.* — The conventional wisdom about ICOs—the meme that drives most headlines—is that explosive valuations were the result of a massive financial bubble. As one leading analyst put it in the *New York Times*, "It's not going to last forever, but it's fun in the interim. The space is giddy right now."[277] A massive financial bubble would certainly help explain why the market didn't seem to care about the investor protections in smart contract code.

The possibility of a bubble accords well with the existing literature on what drives cryptoasset performance. While we are the first to study investor-protection measures found in code, numerous researchers have investigated the relationship between market performance and a host of potential predictors, including founder profiles, business plan characteristics, social media factors, known cybersecurity incidents, and more.[278]

---

273. See Michael Hiltzik, When Grandma and Grandpa Join the Frenzy, You Know Bitcoin is Turning into a Bubble, L.A. Times (Dec. 1, 2017), http://www.latimes.com/business/hiltzik/la-fi-hiltzik-bitcoin-bubble-20171201-story.html (on file with the *Columbia Law Review*).

274. See, e.g., John Omar, Making a Living Day Trading Cryptocurrency, Chain Operator, https://chainoperator.com/making-a-living-day-trading-cryptocurrency/ [https://perma.cc/3EB2-6YEJ] (last updated Sept. 1, 2018).

275. See, e.g., Jacob Hale Russell, Misbehavioral Law and Economics, 51 U. Mich. J.L. Reform 549, 549–54 (2018) (arguing for a normative distinction between taste-driven and mistake-driven irrationality). Things do get complicated for our prejudiced normative priors when it's "grandma and grandpa" who are seeking the thrills. See Peter Rudegeair & Akane Otani, Bitcoin Mania: Even Grandma Wants In on the Action, Wall St. J. (Nov. 29, 2017), https://www.wsj.com/articles/bitcoin-mania-even-grandma-wants-in-on-the-action-1511996653 (on file with the *Columbia Law Review*).

276. See, e.g., Foley et al., supra note 64, at 1.

277. Popper, Easiest Path, supra note 10 (internal quotation marks omitted) (quoting Chris Burniske, an industry analyst). For industry postmortems on the alleged financial bubble, see supra notes 14 and 19.

278. See supra note 31 (describing the existing literature that explores the influence of various factors on market performance).

A consistent theme in this emerging literature is that reputation is the key to understanding the ICO market. Unfortunately, reputation is hackable. For instance, one paper finds that management team quality, as rated on a website called ICObench.com, predicts market performance.[279] ICObench, however, has been accused of operating as a "pay-to-play" operation.[280] Indeed, many rating platforms at the heart of the ICO informational ecosystem[281] operate on a "pay-to-be-rated" model.[282] Project owners place a high value on their project's rating and are willing to pay as much as $20,000 for a rating on the most influential sites.[283] Such paid

279. See Momtaz, supra note 31, at 21, 31 (defining management team quality and calling it a "first-order predictor" for ICO success). But see Rhue, supra note 31, at 22–24 (finding no clear link between rating scores and prices).

280. See Filip Poutintsev, Beware of ICO Bench!, Cryptocurrency Hub (May 13, 2017), https://cryptocurrencyhub.io/beware-of-ico-bench-a41e401b69ea [https://perma.cc/VR3P-2KYA]. As another commentator puts it, "Most incredible of all . . . is just how blatant the greed and corruption exhibited by sites like ICObench has become, so much so that even the Marquis de Sade himself would blush if he were alive today." ICObench Warmer, Tokenicide (Apr. 24, 2017), https://www.tokenicide.com/opinion/icobench-warmer/ [https://perma.cc/2KG3-68GH].

281. See Kai Sedgwick, ICO Trackers Are the New Gatekeepers of Crowdsales, Bitcoin.com (Mar. 22, 2018), https://news.bitcoin.com/ico-trackers-are-the-new-gatekeepers-of-crowdsales/ [https://perma.cc/H2SP-HNFF] [hereinafter Sedgwick, ICO Trackers]; WHA Project, We Are Rated by ICO Bench Experts Now!, Steemit (Sept. 21, 2017), https://steemit.com/cryptocurrency/@whaproject/we-are-rated-by-ico-bench-experts-now [https://perma.cc/URD8-FB95]. Like Yelp, where business owners manage their own Yelp page, the project owners manage everything except the rating on the project's ICO page within the rating site. Any project can submit a request for an ICO page, but the sites reserve the right to deny requests at their discretion. See, e.g., FAQ, ICObench, https://icobench.com/faq [https://perma.cc/9QZZ-JJXE] (last visited Jan. 27, 2019) (describing ICObench's rating system, which combines a rating by the website with ratings by "independent experts"); Publish Your ICO, ICObench, https://icobench.com/publish (on file with the *Columbia Law Review*) (last visited Jan. 27, 2019) (requesting information from ICOs and preICOs wishing to publish pages on ICObench and offering expedited review for a fee). Each rating site also has a unique feature they promote to set them apart from the others. For example, ICObench distinguishes itself with ratings crowdsourced by "independent experts," rather than via the paid promotion model. See Stats and Facts, ICObench, https://icobench.com/stats [https://perma.cc/DQ5R-GB2S] (last visited Mar. 8, 2019). Cryptorated allows users to "upvote" tokens in the queue to be rated and provides both "actual ratings" and "curved ratings" for users to see where a token stands in relation to other ICOs. See ICO Rating System, Cryptorated, https://cryptorated.com/ico-ratings-calculator/ [https://perma.cc/LR9J-8PZG] (last visited Jan. 27, 2019). Others have other features. ICO Drops has an "interest level" weighing short-term conditions, and a "bounty program" that allows users to get tokens by helping the ICO by, for example, promoting it on social media. About Us, ICO Drops, https://icodrops.com/about/ [https://perma.cc/69LZ-WYAD] (last visited Jan. 27, 2019). ICORating organizes its IPOs by ten investment ratings from positive to negative, based on the "independent opinion[s] of ICORating experts." ICORating, http://www.icorating.com [https://perma.cc/BKH2-SJ4Z] (last visited Jan. 27, 2019); Project Evaluation, ICORating, https://icorating.com/methodology/ [https://perma.cc/SF7G-3CPY] (last visited Jan. 27, 2019).

282. See Sedgwick, ICO Trackers, supra note 281.

283. Kirill Shilov, What Should Your ICO Marketing Plan Look Like in 2018?, Hacker Noon (Jan. 16, 2018), https://hackernoon.com/what-should-your-ico-marketing-plan-look-

systems have well-known pathologies, as reflected in the credit-ratings experience during the financial crisis.[284] As a result, when academic papers find that some proxy for social "hype" or "buzz" correlate with higher returns,[285] we are not heartened. Instead, they only make us worry about targeted ads[286] and "pump-and-dump" cartels that coordinate massive social media pushes to temporarily inflate prices before selling their tokens to their marks.[287] These sources of noise and misdirection

---

like-in-2018-315135fe9851 [https://perma.cc/6LXP-9TTQ] (reporting that ICORating charges $20,000 for a report). Altogether, the average cost of advertising packages from top ICO marketing agencies starts at around $280,000. Id.

We had little success independently investigating how much a number of popular rating sites charge. Some rating sites, such as ICO Champs, ICO Drops, and Smith + Crown, disclaim any fee-for-rating service. See Frequently Asked Questions About ICO Champs, ICO Champs, https://www.icochamps.com/#faq-section [https://perma.cc/M83W-KKZ2] (last visited Jan. 27, 2019); Privacy Policy, Smith + Crown, https://www.smithandcrown.com/faq/ [https://perma.cc/EU8F-4FQU] (last visited Jan. 27, 2019); Submit ICO, ICO Drops, https://icodrops.com/submit-ico/ [https://perma.cc/29VF-6EGP] (last visited Jan. 27, 2019). Others have premium models which permit faster listings or access to special platforms in return for payment, such as CoinGecko and ICObench. See How Can I Make My ICO Sponsored?, CoinGecko, https://support.coingecko.com/knowledge_base/topics/how-can-i-make-my-ico-sponsored [https://perma.cc/CG9S-5DLS] (last visited Jan. 27, 2019); Premium, ICObench, https://icobench.com/premium [https://perma.cc/DPG3-R4RM] (last visited Jan. 27, 2019).

Finally, a few popular sites are explicit that they take payment, but sometimes will not disclose how much. For example, ICO Holder requires $500 to be listed. See Publish ICO, ICO Holder, https://icoholder.com/en/v2/ico/create [https://perma.cc/XSK2-AEJZ] (last visited Feb. 5, 2019). On the other hand, CoinSchedule, ICO Alert, ICO Rating, and ICO Watchlist will not disclose their price until after an ICO has been submitted for listing. See Add a New ICO, ICO Watch List, https://icowatchlist.com/add-ico [https://perma.cc/4U6G-XRYX] (last visited Jan. 27, 2019); Consulting, ICO Alert, https://info.icoalert.com/consulting [https://perma.cc/L8FL-RWTG] (last visited Jan. 27, 2019); ICORating Terms and Conditions, ICO Rating, https://icorating.com/terms-and-conditions/ [https://perma.cc/PDT9-38RM] (last visited Feb. 5, 2019); The Ultimate ICO Guide, CoinSchedule, https://www.coinschedule.com/brochure.html (on file with the *Columbia Law Review*) (last visited Jan. 27, 2019) .

284. See Gretchen Morgenson, Ratings Agencies Still Coming Up Short, Years After Crisis, N.Y Times (Jan. 8, 2016), https://www.nytimes.com/2016/01/10/business/ratings-agencies-still-coming-up-short-years-after-crisis.html (on file with the *Columbia Law Review*).

285. See Bourveau et al., supra note 26, at 5; Rhue, supra note 31, at 21–23.

286. See Louise Matsakis, The Cryptocurrency Industry Might Actually Benefit from an Ad Ban, WIRED (Apr. 4, 2018), https://www.wired.com/story/cryptocurrency-industry-might-benefit-from-ad-ban/ [https://perma.cc/W74X-HYAD]; Kate Rooney, Twitter Bans Cryptocurrency Advertising, Joining Other Tech Giants in Crackdown, CNBC (Mar. 26, 2018), https://www.cnbc.com/2018/03/26/twitter-bans-cryptocurrency-advertising-joining-other-tech-giants-in-crackdown.html [https://perma.cc/39SZ-MU8T].

287. See Griffin & Shams, supra note 8; Julian Hosp Tenx, The ICO World Is Full of Pump-and-Dump Schemes—Don't Be a Victim, Venture Beat (Aug. 26, 2017), https://venturebeat.com/2017/08/26/the-ico-world-is-full-of-pump-and-dump-schemes-dont-be-a-victim/ [https://perma.cc/82W4-KUF7]; Oscar Williams-Grut, 'Market Manipulation 101': 'Wolf of Wall Street'-style 'Pump and Dump' Scams Plague Cryptocurrency Markets, Bus. Insider (Nov. 14, 2017), http://www.businessinsider.com/ico-cryptocurrency-pump-and-dump-telegram-2017-11 [https://perma.cc/CZ8Q-JCRL]; see also Erin Griffith,

have contributed to many bubbles in the past.[288]

Of course, reputation-driven markets are not necessarily all bad; it is the particular characteristics of this one that cause concern. We are not alone in this worried hand-wringing. Even researchers who hold out hope that "the wisdom of crowds" might one day triumph still characterize the ICO market as a series of "information cascades" susceptible to insanity.[289] Cooler heads suggest that taking market returns seriously during the 2017–2018 highs would have been seriously misleading, given the market's immaturity and "speculative frenzy."[290] As of early 2019, there is compelling evidence that valuation highs were more bubble than accurate assessments of promising projects. The market capitalization of all cryptocurrencies fell over eighty percent in 2018,[291] and trading of certain coins has essentially stopped completely.[292] Research that identifies the particular sources of air for the bubble will be valuable going forward.[293]

The Hustlers Fueling Cryptocurrency's Marketing Machine, WIRED (June 12, 2018), https://www.wired.com/story/the-hustlers-fueling-cryptocurrencys-marketing-machine/ [https://perma.cc/7YGD-8FKJ] ("Much of the [crypto] industry's action happens on a messaging app called Telegram."); Deep Patel, 6 Red Flags of an ICO Scam, TechCrunch (Dec. 7, 2017), https://techcrunch.com/2017/12/07/6-red-flags-of-an-ico-scam/ [https://perma.cc/8PUY-WSPB] (describing Reddit sub-threads' discussions of specific ICOs as a good source for technical evaluations of crypto projects).

288. See Erik F. Gerding, Law, Bubbles, and Financial Regulation 63–99 (2014).

289. Lee et al., supra note 31, at 23, 30–31 (acknowledging that the "insanity of crowds" might be at work).

290. See Howell et al., supra note 26, at 4 n.3 ("[I]n light of the sector's immaturity and speculative frenzy, returns appear more divorced from the goal of serious utility token issuers to use the ICO to (a) raise financing; and (b) promote customer adoption of their networks.").

291. See Ryan Browne, Cryptocurrencies Have Shed Almost $700 Billion Since January Peak, CNBC (Nov. 23, 2018), https://www.cnbc.com/2018/11/23/cryptocurrencies-have-shed-almost-700-billion-since-january-peak.html [https://perma.cc/E29M-97AF] (tracking a decline in total cryptocurrency market capitalization to $138.6 billion, from a peak of over $830 billion in the beginning of 2018).

292. See Deceased Coins, Dead Coins, https://deadcoins.com/ [https://perma.cc/Z4KF-99BE] (last visited Jan. 27, 2019) (listing 680 cryptocurrencies as "deceased," along with another 182 as "scams"); see also Jay Adkission, The Cryptocurrency Paradox and Why Crypto Is Failing, Forbes (Nov. 28, 2018), https://www.forbes.com/sites/jayadkisson/2018/11/28/the-cryptocurrency-paradox-and-why-crypto-is-failing/ [https://perma.cc/2SFY-AWNS] (describing the "vast majority" of cryptocurrencies as having failed).

293. We have observed a number of instances in which reports of market capitalization greatly exceed what we have been able to identify on blockchain explorers like etherscan.io. Theoretically, investors could determine how many tokens were provided to how many investors during an ICO and in exchange for what kind of consideration. The number of transactions should correspond to the number of buyers. Verifying the size of a team's ICO looks like a mathematical exercise: The product of the number of tokens sold and the price paid. In practice, however, this kind of analysis is impractical. First, teams routinely engage in private, individualized sales of their tokens to specific investors outside of the blockchain. See Applicature, Private Sale or Public Sale?, Medium (Nov. 8, 2018),

In a sense, a bubble would be the least surprising and most manageable explanation of the ICO market's rapid price swings. Regulators would need to focus on the time-honored, if difficult task of popping future bubbles with better informational requirements. But the "animal spirits" of irrational exuberance are not the only plausible drivers of ICO demand.[294]

2. *Illicit Demand.* — As a complement to the bubble theory of cryptoasset success, many signs suggest that a material portion of cryptoasset demand is driven by money launderers, tax evaders, and other holders of illicit cash.[295] Some of these illicit holders might be

---

https://medium.com/applicature/private-sale-or-public-sale-b515476718a3 [https://perma.cc/S7N7-KTUP] ("Presaling coins of a cryptocurrency or token of a blockchain project has become an effective method of raising funds for the development of a new application."). Though it is possible to verify that a project's tokens were transferred to certain wallets at some point before its public sale, there is no way to know how much the owners of those wallets actually paid for the tokens. Maybe unsurprisingly, the self-reported size of a team's private presale often dwarfs the amount sold in its ICO. Thus, for instance, though Paragon announced its launch with a $50 million capital raise including presale placements, the SEC recently entered into a consent judgment finding only around $12 million in total was raised. See supra note 174.

Second, there is generally no way to link a given Ethereum wallet address to a specific person or institution. See Dominiek Ter Heide, A Closer Look at Ethereum Signatures, Hacker Noon (Feb. 16, 2018), https://hackernoon.com/a-closer-look-at-ethereum-signatures-5784c14abecc [https://perma.cc/4EEB-TUAT] ("The notion of an account is a bit of a misnomer, because in strict technical terms there are only keys and a ledger of funds that correspond with those keys."); cf. Sudhir Khatwani, 6 Ways to Guarantee Anonymity When Making Bitcoin Transactions, Coin Sutra (Nov. 10, 2018), https://coinsutra.com/anonymous-bitcoin-transactions/ [https://perma.cc/BX83-QGBH] ("Bitcoin transactions, by design, are not linked to a person or identity . . . . A person's name, physical address, or email is found nowhere in the transaction."). Ethereum addresses can be created rapidly and for free. See, e.g., Create New Wallet, MyEtherWallet, https://www.myetherwallet.com/ (on file with the *Columbia Law Review*) (allowing users to instantly generate an Ethereum wallet address at no cost). As a result, though it's possible to verify that a certain number of Ethereum addresses received a project's tokens, it's impossible to confirm that a certain number of investors participated in the sale. A development team seeking to drive up enthusiasm for its token might spawn a high number of wallet addresses and then transfer tokens to them. These transactions would be indistinguishable from legitimate arm's-length purchases by actual investors. As a result, even the portion of an ICO that takes place on a blockchain is subject to manipulation.

294. See generally Donald C. Langevoort, Taming the Animal Spirits of the Stock Markets: A Behavioral Approach to Securities Regulation, 97 Nw. U. L. Rev. 135 (2002) (offering a behavioral approach to irrational markets).

295. See Omri Marian, Are Cryptocurrencies Super Tax Havens?, 112 Mich. L. Rev. First Impressions 38, 43–44 (2013), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1001&context=mlr_fi [https://perma.cc/L3RZ-G5L2] ("Tax-evaders and money launderers regularly use . . . tactics to attempt to hide the sources, as well as the destination, of funds."); Ryan Clements, Decoding the Demand for Cryptocurrency: What Is Driving the Historic Price Surge?, FinReg Blog (Sept. 26, 2017), https://sites.duke.edu/thefinregblog/2017/09/26/decoding-the-demand-for-cryptocurrency-what-is-driving-the-historic-price-surge/ [https://perma.cc/7VGU-PSQN] ("Another reason for the run up in price of cryptocurrencies . . . is its ability to facilitate criminal activity and to make transactions anonymously—away from the informational reach of government and regulators.").

inspired by the original, anarcho-capitalist vision for Bitcoin: to "win a major battle in the arms race and gain a new territory of freedom" from centralized governments.[296] Others might not have politics on their mind.

This second piece of "conventional wisdom" about the cryptoasset market was initially suggested by accounts of how Bitcoin's growth was fueled by the drug trade.[297] Recent allegations that Russian hacking of the Democratic National Committee in 2016 was bought and paid for using Bitcoin have made this concern more salient.[298] Indeed, one recent paper found that approximately *half* of all bitcoin transactions were associated with some form of illegal activity.[299] Another found that the imposition of "Know Your Customer" policies designed to enforce tax and anti-money laundering laws shrank ICO returns.[300]

This source of demand would have entirely different implications for ICO regulation than the "bubble" story. Obviously, it would seriously weaken the case for ensuring an "innovation-friendly" environment through well-tailored regulation. It would also counsel in favor of greatly increasing scrutiny on the major players in an ICO ecosystem who are benefiting from their dalliance with criminal underworlds.

Along with the "bubble demand" hypothesis, the "illicit demand" hypothesis also comports with some of our results. For instance, if criminal payments facilitation is indeed a major driver of demand for ICOs, then it is unsurprising that investors do not seem to care about whether founder vesting promises are delivered via smart contract code. Instead, they might simply be treating all ICOs like new printings of black-market money. If this is the case, then the high-flying business plans found in ICO whitepapers are merely window dressing, or an initial spark to help create a network effect for a new cryptocurrency. This form of demand could dovetail with the speculators driving the bubble described above. And it seems fair to say that gamblers, bubble speculators, and

---

296. Email from Satoshi Nakamoto to the Cryptography Mailing List, Re: Bitcoin P2P E-Cash Paper (Nov. 7, 2008), https://www.mail-archive.com/cryptography@metzdowd.com/msg09971.html [https://perma.cc/R8TL-PXRU].

297. See Reza Raeesi, The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can This Storm Be Weathered?, 8 Glendon J. Int'l Stud., 2015, at 1, 2, 9 (noting that for a time, between 4.5% and 9% of all Bitcoin transactions were connected to the Silk Road, an online black market associated with trade in illegal drugs).

298. See Jordan Pearson, The Russians Who Allegedly Hacked the DNC Mined Bitcoin to Fund Their Operation, Motherboard (July 13, 2018), https://motherboard.vice.com/en_us/article/bjbz7v/russian-hackers-mined-bitcoin-mueller-indictment [https://perma.cc/8JHL-8L4R].

299. See Foley et al., supra note 64, at 2 ("For example, approximately one-quarter of all users (26%) and close to one-half of bitcoin transactions (46%) are associated with illegal activity.").

300. See Lee et al., supra note 31, at 3 ("[A]nti-money laundering measures, such as a Know Your Customer policy, negatively predict fundraising success.") .

criminal cartels alike will not be inordinately attentive to smart contract code.

3. *Crypto Winnings*. — A third possible source of ICO demand might be coming from investors who raked in gains on investments in Bitcoin and Ethereum. These two cryptocurrencies have appreciated enormously since the beginning of 2015. This has led to massive wealth-creation for a cohort of so-called "Bitcoin millionaires,"[301] and their decisions about what to do with their winnings might be driving a fair bit of ICO success.

This hypothesis might play out in two ways. First, ICOs might serve as a decent place to park winnings that are trapped in crypto purgatory. To the extent that the "crypto winners" have been the illicit actors described above, they will have trouble converting their cryptocurrency holdings to fiat money through traditional channels. To be explicit, even if they could easily turn ether or Bitcoin directly into cash, they might not want to—they might be worried that governments would investigate the owners of fiat cash hoards.

Instead, they might attempt to wait until cryptocurrency affords them more access to consumption in the real world. In doing so, ICOs would provide a reasonably good vehicle through which to diversify their holdings and to attempt to invest their winnings in potentially lucrative ventures.

Second, to the extent that some investors treat cryptoasset markets like casinos, they might be simply gambling with the house's money.[302] That is, it is easier to imagine investing in speculative assets, without caring too much about the details, when the stake one uses to invest with is itself the product of recent, sharp, gains. This is why people sometimes (foolishly) play the roulette wheel after winning at blackjack at the casino.

The "crypto winnings" hypothesis is the least-explored in literature about ICO demand and market performance. Nevertheless, there is preliminary evidence supporting it. Specifically, one time-series analysis suggests that blockbuster ICOs have negative effects on Bitcoin and ether prices.[303] This suggests that investors are trading between ether and Bitcoin on the one hand, and ICOs, on the other. Other analysts observe that ICO teams who amassed huge Ethereum war chests from the proceeds of their token sales were eventually forced to liquidate them as the price of ether dropped. This intensified price declines in not only ether but tokens as well.[304] If research continues to bear out this effect, it

---

301. See Don Reisinger, Newly-Minted Bitcoin Millionaires Are Lining Up to Buy Lamborghinis, Fortune (Apr. 3, 2018), http://fortune.com/2018/04/03/bitcoin-millionaire-lamborghini-when-lambo/ [https://perma.cc/7AXD-EMUL].

302. See, e.g., Derek A. Dion, Note, I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash, 2013 U. Ill. J.L. Tech. & Pol'y 165, 187 (noting the extent of gambling linked to Bitcoin).

303. See Masiak et al., supra note 31.

304. See, e.g., Angel Reyes, Ethereum ICO Funds Liquidation Reaches All-Time High as December Ends, Crypto.IQ (Dec. 31, 2018), https://cryptoiq.co/ethereum-ico-funds-liquidation-reaches-all-time-high-as-december-ends/ [https://perma.cc/GQT4-B2XV]; Joseph

would only further support the kinds of regulatory responses that are appropriate in light of the "bubble" and "illicit demand" scenarios described above.

4. *Smart Money.* — Finally, it is possible that some ICO demand is driven by legitimately smart money. Anecdotal reports indicate that a wide range of old-growth VC firms, hedge funds, and family offices are, in fact, investing in ICOs.[305] Sometimes, they invest directly, as with the participation of Sequoia Capital, Andreessen Horowitz, and Union Square Ventures in the Filecoin ICO.[306] In other cases, they invest through intermediaries, whether due to regulatory restrictions on their holdings, or simply to work with other investors who are experts in the cryptoasset class.[307] In either case, these investors are the most likely to be engaging in fundamental analysis of ICOs, and thus the most likely to be scrutinizing smart contract code.

The presence of these investors in the market raises numerous questions for researchers and regulators alike. First, recall the colloquy with the ICO advocate in Part IV.A above. In a world where the code of "lex cryptographica" is not performing crucial investor-protection roles, we must look to traditional sources of protection. One of those is public regulation, but another is private gatekeeping. In the IPO world, for instance, the involvement of initial underwriters and primary market-makers channels pricing toward a fundamental valuation.[308] So, too, does the participation of institutional investors on the long and short sides of the market.[309] These investors do the heavy analytical lifting that helps

---

Young, Did ICOs Cause Ethereum to Drop by 44% in 2 Weeks by Dumping on the Market?, CCN (Aug. 14, 2018), https://www.ccn.com/did-icos-cause-ethereum-to-drop-by-44-in-2-weeks-by-dumping-on-the-market/ [https://perma.cc/D3Q7-7UVW]; c.f. Larry Cermak, ICOs Are Not Liquidating Their ETH Treasuries, Despite Price Declines. Yet., The Block (Nov. 20, 2018), https://www.theblockcrypto.com/2018/11/20/icos-are-not-liquidating-their-eth-treasuries-despite-price-declines-yet/ [https://perma.cc/K9SX-HDKM].

305. See, e.g., Maiya Keidan & Jemima Kelly, Number of Crypto Hedge Funds Surges Amid Bitcoin Volatility, Reuters (Feb. 15, 2018), https://www.reuters.com/article/uk-hedgefunds-bitcoin/number-of-crypto-hedge-funds-surges-amid-bitcoin-volatility-idUSKCN1FZ189 [https://perma.cc/UZN3-E729]; Olga Kharif & Camila Russo, Venture Capital Surges into Crypto Startups, Bloomberg (Mar. 26, 2018), https://www.bloomberg.com/news/articles/2018-03-26/icos-can-wait-venture-capital-surges-into-crypto-startups [https://perma.cc/3UQ5-66AM].

306. See Fitz Tepper, Filecoin's ICO Opens Today for Accredited Investors After Raising $52M from Advisers, TechCrunch (Aug. 10, 2017), https://techcrunch.com/2017/08/10/filecoins-ico-opens-today-for-accredited-investors-after-raising-52m-from-advisers/ [https://perma.cc/YWN9-NY3H].

307. See, e.g., Michael McDonald, Cryptocurrency Hedge Fund BlockTower Raises $140 Million, Bloomberg (Jan. 4, 2018), https://www.bloomberg.com/news/articles/2018-01-04/cryptocurrency-fund-blocktower-is-said-to-raise-140-million [https://perma.cc/YP55-E2Y3].

308. Steven E. Bochner, Jon C. Avina & Calise Y. Cheng, Wilson Sonsini Goodrich & Rosati, Guide to the Initial Public Offering 18–20 (8th ed. 2016), https://www.wsgr.com/publications/PDFSearch/IPOGuide2016.pdf [https://perma.cc/SFK6-8RF4].

309. See id. at 29.

protect retail investors from succumbing to irrationality. And (most of the time) these investors *read the investment contracts*.[310]

Are "smart money" investors playing similar channeling roles in the ICO market? It is hard to say. Maybe investors like Sequoia Capital are entering into side letters with ICO teams to contractually ensure that supply and vesting promises are upheld.[311] Maybe the Andreessen Horwitzes of the world are scrutinizing modifiability and holding private corporate-governance fiduciary powers to rein in its use. They might also be embedding important information into market prices—for instance, information about ICO project activity, founding team reputation, and the quality of an ICO's informational disclosures.[312] On the other hand, maybe they're not. There is nothing stopping the "smart money" from riding cryptoasset volatility for all it's worth. Bubbles are profitable for smart money, too, so long as they can cash out before the music stops. It would be valuable for future research to suss out the strategies and tactics that old-growth investors have been employing in this market.

From a regulatory perspective, the presence of smart money presents both a reason to care about preserving ICOs as a potentially valuable innovation and a potential lever to use. Indeed, one happy story that might be told a decade hence is that the ICO market of 2017 merely represented a period of growing pains, where reliable information sources and reputable gatekeepers were taking formation.

C. *Whose Market Might It Become?*

Based on the strong evidence that smart money is *not* leading this market, it can be tempting to cast doubt on all aspects of ICOs, including smart contracts. Though it will take future research to prove it, the ICO buy side today looks to us like a mixture of a bubble and an illicit market, with some smart money in the mix. And yet, this doesn't mean that smart contracts are meaningless.

As John Maynard Keynes (didn't) say, "The market can stay irrational longer than you can stay solvent."[313] But over a long enough time horizon,

---

310. Cf., e.g., Matt Levine, You Can't Always Read the Documents, Bloomberg (June 5, 2018), https://www.bloomberg.com/opinion/articles/2018-06-05/you-can-t-always-read-the-documents (on file with the *Columbia Law Review*) (explaining that arbitrageurs are the people who "read[] the bond documents so that everyone else doesn't have to. It's just that everyone else pays [them] to do it.").

311. The Storj secondary vesting contract, discussed infra at note 627, would provide a different (and more transparent) way to accomplish the same end.

312. Notably, it is possible to short cryptoassets through some exchanges. It is unclear how broad or sophisticated the practice is. It certainly seems reasonable to suggest that shorting crypto is not as strong a mechanism for embedding contrarian views or information into prices as it is in securities and commodities markets.

313. See Jason Zweig, Keynes: He Didn't Say Half of What He Said. Or Did He?, Wall St. J.: Marketbeat (Feb. 11, 2011), https://blogs.wsj.com/marketbeat/2011/02/11/keynes-he-didnt-say-half-of-what-he-said-or-did-he/ [https://perma.cc/N5HY-W5JA].

every bubble must pop. This leaves open the possibility that fundamental aspects of smart contract quality will, eventually, sway the outcomes of the market, with smart money at the helm.

In many ways, the ICO market of the past couple of years resembles the dot-com boom that took place at the end of the last century. That boom featured massive reallocations of investment capital toward nearly any company that proposed a business strategy that incorporated what was then called the "world wide web."[314] The same has been observed in relation to "blockchain" and "token"-based business plans in today's climate.[315] In the dot-com boom, investors also broke from fidelity to traditional investment metrics like price-to-earnings ratios, instead relying on new valuation drivers like the sheer number of "eyeballs" viewing a website or the "stickiness" of the website experience.[316] Short-term performance on these metrics turned out to have little relation to a company's long-term success.[317]

It is hard not to see the rise of crypto-investment metrics like GitHub reputational stars, Twitter followers, and Instagram likes as representing a similarly problematic set of proxies for the possibility of network success. Financially, between the years of 1997 and 2000, internet stocks zoomed up and up, suggesting a new paradigm for corporate finance. The cryptoasset investor subcultures devoted to rejecting "fear, uncertainty, and doubt" may be in for a similarly painful fall to earth. Almost without question, both the dot-com market and the ICO market would have benefited from clearer and more reliable information environments to curb their excesses.

And yet, from a distance of twenty years, the economic follies of the late 1990s look less like utter madness, and more like a kind of overeager prescience. The clothing retailer boo.com may have gone belly-up, but e-commerce represents 40% of sales for even classic footprint companies like J.Crew,[318] and leading apparel startups like Everlane and Rent the Runway are decidedly "online-native."[319] And though the grocery deliverer Webvan.com was widely derided as one of the biggest flops of

---

314. See Elizabeth Demers & Baruch Lev, A Rude Awakening: The Internet Shakeout in 2000, 6 Rev. Acct. Stud. 331, 335 (2001).

315. See, e.g., Nicole Bullock & Robin Wigglesworth, Blockchain Fervour Evokes Memories of Dotcom Bubble, Fin. Times (Dec. 18, 2017), https://www.ft.com/content/40ec964a-e429-11e7-8b99-0191e45377ec (on file with the *Columbia Law Review*).

316. See id.

317. See id.

318. See J. Crew, Revenues & Sales, eMarketer Retail, https://retail-index.emarketer.com/company/data/5374f24d4d4afd2bb444660d/5374f2814d4afd824cc159d6/lfy/false/jcrew-revenues-sales [https://perma.cc/REP5-PENE] (last visited Jan. 27, 2019).

319. See Everlane, https://www.everlane.com/ [https://perma.cc/6EX7-DYJ3] (last visited Jan. 27, 2019); Rent the Runway, https://www.renttherunway.com/ [https://perma.cc/J2AV-ESGC] (last visited Jan. 27, 2019).

the dot-com bust,[320] Amazon is pushing in that direction.[321] The rush for eyeballs has become a rush for data, and online shopping continues its remarkably paced growth.[322]

Will we look back on the cryptoasset craze initiated in 2017 with similar curiosity twenty years from now? What will fall away as the ephemera of the moment, and what will work itself deeply into our economic institutions? Given the froth of the market, it can be tempting to focus on the gut-level question of whether the ICO market is a financial bubble, and if so, how regulators should address it.

But our view is that legal policymakers might do well to look beyond the bubble (and its certain fate). Bubbles misallocate capital to unproductive uses and divert the energy of those who respond to the capital's call. They also harm unsavvy investors who fall prey to the salesmen who are selling a bull market.[323] These animal spirits cause huge amounts of mischief. It ought to be—and indeed is—the province of lawmakers and regulators to temper them.[324] And yet, we are convinced there is something useful to be learned from this first experiment in blockchain governance. Some firms *are* encoding their promises, though it's not obviously rewarding to do so. Others are working to create intermediaries and certification regimes despite the contrary incentives present in a sharply rising market. Rewarding such good actors should be as important to regulators as punishing fraudsters.

---

320. See 10 Big Dot.com Flops: Webvan.com, CNN Money, http://money.cnn.com/galleries/2010/technology/1003/gallery.dot_com_busts/2.html [https://perma.cc/8BPW-B8A2] (last visited Jan. 27, 2019) (describing Webvan as the biggest flop of the dotcom bubble).

321. See Nick Turner, Selina Wang & Spencer Soper, Amazon to Acquire Whole Foods for $13.7 Billion, Bloomberg (June 16, 2017), https://www.bloomberg.com/news/articles/2017-06-16/amazon-to-acquire-whole-foods-in-13-7-billion-bet-on-groceries (on file with the *Columbia Law Review*).

322. See Ali Hortaçsu & Chad Syverson, The Ongoing Evolution of US Retail: A Format Tug-of-War, 29 J. Econ. Persp. 89, 96 (2015) (putting e-commerce in context and documenting its nominal eleven-fold increase between 2000 and 2014).

323. See Sean Silverthorne, Inexperienced Investors and Market Bubbles, Harvard Bus. Sch.: Working Knowledge (Feb. 19, 2007), https://hbswk.hbs.edu/item/inexperienced-investors-and-market-bubbles [https://perma.cc/TT8D-XUM6].

324. One implication of our Article is that regulatory agencies might investigate the costs and benefits of requiring that cryptocurrencies match their marketing materials to their smart contracts. For further recommendations on potential disclosure requirements, see generally Chris Brummer, Trevor Kiviat & Jai R. Massari, What Should Be Disclosed in an Initial Coin Offering?, *in* Cryptoassets: Legal and Monetary Perspectives (forthcoming 2019) (on file with the *Columbia Law Review*); Usha Rodrigues, Semi-Public Offerings? Pushing the Boundaries of Securities Law (Univ. of Ga. Sch. of Law Legal Studies Research Paper No. 2018-30, 2018), https://ssrn.com/abstract=3242205 (on file with the *Columbia Law Review*).

CONCLUSION

The computer code at the heart of ICOs enables a new way of founding and governing enterprises. It allows entrepreneurs to adopt the ICO method, whether for good or ill. But while smart contract technology may be a driver—indeed, a definitional component—of the ICO phenomenon, we believe our study demonstrates in detail that smart contracts are also embedded in the social world. Just like Coca-Cola's vending machines, ICOs are products of their time and place. They are built atop innovative "technical systems" that only recently came into being, and they are conducted within particular "communities of discourse" that happen to exist here and now.[325] To make sense of the technology's role, scholars and regulators alike should study the unique forms that this embeddedness takes.

Our study demonstrates that the current structures—markets, formal organizations, and professional communities—where ICOs take place are producing a disconnect. Far from replacing (or seamlessly extending) law and norms, code is often falling short of expectations. It sometimes fails to deliver key investor protections, and can provide founders with significant, undisclosed authority to alter the terms of investor engagement. While ICOs are promoted by an industrial community that espouses technolibertarian beliefs in the power of "trustless trust" and carefully designed code, actual ICO practices do not uphold that ideology.

The disconnect we observe reflects the informality of the ICO world. Paper contracts and IPOs are joint products of law firms, investment banks, regulators, and a panoply of buy-side institutional intermediaries. Smart contracts and ICOs, at least at the moment, largely result from coders and entrepreneurs working at greater distance from risk-averse gatekeepers. Befitting their relatively informal production setting, smart contracts have been plagued with quality control problems. They suffer vast amounts of hacking,[326] and, as we show, standards as to how code is produced and made legible are wanting.[327] Unlike the traditional legal world, there are currently no guilds or expert institutions governing smart contract coders' practices to encourage quality. To withstand market ups and downs, the ICO community should invest in developing reliable institutions and promulgating best practices for the long term.

The informality of smart contract production leads to risks, to be sure, but it also breeds creativity. Lawyers tend to recycle language from agreement to agreement without much thought, but the smart contract community is full of "makers," excitement, and avocational energy. This distinction suggests that the rate of innovation within smart contracting

---

325. See Suchman, supra note 24, at 92.

326. See Irrera, More Than 10 Percent, supra note 258 ("More than 10 percent of funds raised through 'initial coin offerings' are lost or stolen in hacker attacks.").

327. See supra Part III.

is driven by social factors, as well as technological ones.[328] It also suggests that whether or not the ICO market is a bubble, professionals and hobbyists working on ICOs will be able to port smart contract governance into new settings over the years to come. As their ranks increase, the "no-reading" problem for smart contracts might also be tempered. Right now, one aspect of the disconnect we've identified is that so few people *can* read smart contracts. The community of people who are able to vet and audit smart contracts has much room to grow. As it does grow, and as existing institutions develop vetting capacity, we would expect to see quality improve.

We think that optimal regulation depends heavily on a better understanding of the buy side of the market. But whatever the fraction of investors who deserve protecting, our results show that computer code is not presently a reliable part of the ICO form. Our results strongly suggest that an increased presence of gatekeepers and regulators might help that process along. The SEC, with its newly developed "Cyber Unit,"[329] is increasingly active in patrolling the scene. Other regulators, along with courts, will also contribute to increasing formalization of ICO code standards. So, too, will private standard-setting organizations within the industry itself. The rise of trusted intermediaries will be the next necessary step in any maturation of this novel financial form.

---

328. Cf. Kevin Davis, Contract as Technology, 88 N.Y.U. L. Rev. 83, 86–88 (2013) (encouraging scholars to study innovation in contracting outside traditional domains).

329. See Press Release, SEC, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176 [https://perma.cc/PVR2-3S3N].

APPENDIX A: SUMMARY OF TOP 50 2017 ICOS[330]

ICO Name	**Country**[331]	**Announced Raise ($M)**[332]	**ICO Date**[333]	**Initial Market Value ($M)**[334]	**Market Value 12/31/18 ($M)**[335]
Filecoin	USA[336]	$257.0[337]	9/10/17[338]	N/A[339]	N/A[340]
Tezos	USA[341]	$232.0[342]	7/13/17[343]	$1,138.6[344]	$281.0[345]
EOS Stage	USA[346]	$185.0[347]	6/11/17[348]	$654.9[349]	$2,326.3[350]

330. We first developed the list of projects from www.coinschedule.com. By early 2019, that site no longer provided the relevant data. This chart thus uses a combination of other sources, primarily www.icomarks.com and www.coinmarketcap.com.

331. This column represents the country with which each ICO is associated. Countries are abbreviated using their International Organization for Standardization Alpha-3 code abbreviations.

332. This column represents the total amount of capital raised through each ICO, as reported by publicly available sources.

333. This column represents the last day of the ICO period for each ICO.

334. This column represents the first reported market capitalization for each ICO. The date is different for each ICO and is indicated parenthetically.

335. This column represents the reported market capitalization for each ICO as of December 31, 2018.

336. Filecoin, ICOmarks, http://icomarks.com/ico/filecoin [http://perma.cc/4QH2-8U6M] (last visited Jan. 24, 2019).

337. Id.

338. Id.

339. Filecoin, CoinMarketCap, http://coinmarketcap.com/currencies/filecoin/historical-data/ [http://perma.cc/39NT-7VYN] (last visited Jan. 24, 2019) (showing that no market capitalization has yet been announced).

340. Id.

341. Tezos, ICOmarks, http://www.icomarks.com/ico/tezos [http://perma.cc/5SF2-2PTG] (last visited Jan. 24, 2019).

342. Id.

343. Id.

344. Tezos, CoinMarketCap, http://coinmarketcap.com/currencies/tezos/historical-data/?start=20130428&end=20190124 [http://perma.cc/8MLC-GLCE] (last visited Jan. 24, 2019) (reported as of July 4, 2018).

345. Id.

346. EOS, ICOmarks, http://icomarks.com/ico/eos [http://perma.cc/VW96-QA8H] (last visited Jan. 24, 2019).

347. Id.

348. Id.

349. EOS, CoinMarketCap, http://coinmarketcap.com/currencies/eos/historical-data/?start=20130428&end=20190124 [http://perma.cc/T476-LAY2] (last visited Jan. 24, 2019) (reported as of July 3, 2017).

350. Id.

Paragon	RUS[351]	$50.0[352]	10/15/17[353]	$18.7[354]	$10.9[355]
Bancor	ISR[356]	$153.0[357]	6/12/17[358]	$98.8[359]	$38.6[360]
Kin	CAN[361]	$98.0[362]	9/26/17[363]	$88.0[364]	$28.7[365]
Status	CHE[366]	$100.0[367]	6/20/17[368]	$194.9[369]	$59.8[370]
Tron	CHN[371]	$70.0[372]	9/2/17[373]	$29.3[374]	$1,254.5[375]

351. Paragon Coin, ICOmarks, http://icomarks.com/ico/paragon-coin [http://perma.cc/Z3N6-XMUX] (last visited Jan. 24, 2019).

352. Id.

353. Id.

354. Paragon, CoinMarketCap, http://coinmarketcap.com/currencies/paragon/historical-data/?start=20130428&end=20190124 [http://perma.cc/4GJL-GA8T] (last visited Jan. 24, 2019) (reported as of Nov. 5, 2017).

355. Id.

356. Bancor, ICOmarks, http://icomarks.com/ico/bancor [http://perma.cc/V3WG-H2PG] (last visited Jan. 24, 2019).

357. Id.

358. Id.

359. Bancor, CoinMarketCap, http://coinmarketcap.com/currencies/bancor/historical-data/?start=20130428&end=20190124 [http://perma.cc/MG9S-9DN5] (last visited Jan. 24, 2019) (reported as of June 26, 2017).

360. Id.

361. Kin, ICOmarks, http://icomarks.com/ico/kin [http://perma.cc/EWX2-XU5G] (last visited Jan. 24, 2019).

362. Id.

363. Id.

364. Kin, CoinMarketCap, http://coinmarketcap.com/currencies/kin/historical-data/?start=20130428&end=20190124 [http://perma.cc/J7HA-3LR7] (last visited Jan. 24, 2019) (reported as of Sept. 27, 2017).

365. Id.

366. Status, ICOmarks, http://icomarks.com/ico/status [http://perma.cc/Y4HV-3PU7] (last visited Jan. 24, 2019).

367. Id.

368. Id.

369. Status, CoinMarketCap, http://coinmarketcap.com/currencies/status/historical-data/?start=20130428&end=20190124 [http://perma.cc/W4PJ-PT2D] (last visited Jan. 24, 2019) (reported as of June 28, 2017).

370. Id.

371. Tron, CoinGecko, http://www.coingecko.com/en/ico/tron [http://perma.cc/R5RQ-HSNF] (last visited Jan. 24, 2019).

372. Id.

373. Id.

374. Tron, CoinMarketCap, http://coinmarketcap.com/currencies/tron/historical-data/?start=20130428&end=20190124 [http://perma.cc/ZK8P-KVGX] (last visited Jan. 24, 2019) (reported as of Sept. 28, 2017).

375. Id.

TenX	SGP[376]	$80.0[377]	6/24/17[378]	$115.4[379]	$28.3[380]
MobileGo	USA[381]	$53.0[382]	5/25/17[383]	$139.2[384]	$51.3[385]
KyberNetwork	SGP[386]	$49.0[387]	9/15/17[388]	$254.8[389]	$20.6[390]
MCAP	USA[391]	$44.3[392]	5/7/17[393]	$29.9[394]	$0.1[395]
Loopring	CHN[396]	$45.0[397]	8/16/17[398]	$42.4[399]	$31.5[400]

376. TenX, ICOmarks, http://icomarks.com/ico/tenx [http://perma.cc/U8ZQ-CD8B] (last visited Jan. 24, 2019).

377. Id.

378. Id.

379. TenX, CoinMarketCap, http://coinmarketcap.com/currencies/tenx/historical-data/?start=20130428&end=20190124 [http://perma.cc/7MY3-YVDB] (last visited Jan. 24, 2019) (reported as of July 8, 2017).

380. Id.

381. MobileGo, ICOmarks, http://icomarks.com/ico/mobilego [http://perma.cc/DH2Z-L58N] (last visited Jan. 24, 2019).

382. Id.

383. Id.

384. MobileGo, CoinMarketCap, http://coinmarketcap.com/currencies/mobilego/historical-data/?start=20130428&end=20190124 [http://perma.cc/W5B2-6EBZ] (last visited Jan. 24, 2019) (reported as of June 13, 2017).

385. Id.

386. KyberNetwork, ICOmarks, http://icomarks.com/ico/kybernetwork [http://perma.cc/AKN3-CJQA] (last visited Jan. 24, 2019).

387. Id.

388. Id.

389. Kyber Network, CoinMarketCap, http://coinmarketcap.com/currencies/kyber-network/historical-data/?start=20130428&end=20190124 [http://perma.cc/XAS8-NCZS] (last visited Jan. 24, 2019) (reported as of Sept. 24, 2017).

390. Id.

391. MCAP, ICOmarks, http://icomarks.com/ico/mcap [http://perma.cc/693A-REQS] (last visited Jan. 24, 2019).

392. Id.

393. Id.

394. MCAP, CoinMarketCap, http://coinmarketcap.com/currencies/mcap/historical-data/?start=20130428&end=20190124 [http://perma.cc/T94G-5BF5] (last visited Jan. 24, 2019) (reported as of June 3, 2017).

395. Id.

396. Loopring, ICOmarks, http://icomarks.com/ico/loopring [http://perma.cc/H9CM-FJMU] (last visited Jan. 24, 2019).

397. Id.

398. Id.

399. Loopring, CoinMarketCap, http://coinmarketcap.com/currencies/loopring/historical-data/?start=20130428&end=20190124 [http://perma.cc/UM7V-4KJY] (last visited Jan. 24, 2019) (reported as of Sept. 2, 2017).

400. Id.

Enigma	USA[401]	$45.0[402]	9/11/17[403]	$51.9[404]	$21.6[405]
ICON	JPN[406]	$45.0[407]	9/22/17[408]	$1,976.4[409]	$112.0[410]
PeerBanks	USA[411]	$42.6[412]	9/22/17[413]	N/A[414]	N/A[415]
Electroneum	GBR[416]	$40.0[417]	10/20/17[418]	$349.8[419]	$64.0[420]
Aeternity	BGR[421]	$24.4[422]	6/19/17[423]	$100.6[424]	$90.6[425]

401. Enigma, ICOmarks, https://www.icomarks.com/ico/enigma-catalyst [https://perma.cc/R2TX-CGSR] (last visited Feb. 2, 2019).

402. Id.

403. Id.

404. Enigma, CoinMarketCap, http://coinmarketcap.com/currencies/enigma/historical-data/?start=20130428&end=20190124 [http://perma.cc/UEH8-2TXE] (last visited Jan. 24, 2019) (reported as of Oct. 14, 2017).

405. Id.

406. ICON, ICOmarks, https://www.icomarks.com/ico/icon [https://perma.cc/3CM9-7T7X] (last visited Feb. 2, 2019).

407. Id.

408. Id.

409. ICON, CoinMarketCap, http://coinmarketcap.com/currencies/icon/historical-data/?start=20130428&end=20190124 [http://perma.cc/XAG7-SKYF] (last visited Jan. 24, 2019) (reported as of Dec. 25, 2017).

410. Id.

411. PeerBanks, ICOmarks, https://www.icomarks.com/ico/peerbanks [https://perma.cc/GJ5N-GLVX] (last visited Feb. 2, 2019).

412. Id.

413. Id.

414. No market capitalization data for PeerBanks were available from publicly available coin-focused websites because PeerBanks has not yet been listed on an exchange. See PeerBanks IRA (@PeerBanks), Twitter (Feb. 8, 2018), https://twitter.com/PeerBanks/status/961816827281080321 [https://perma.cc/4TW3-ZJSQ] ("We continue waiting for the transfers of your peerbanks to our waves wallet, please, until this does not end, we will not be able to advance to the next step, which is to place Peerbanks IRA in an exchange.").

415. See supra note 414.

416. Electroneum, ICOmarks, https://www.icomarks.com/ico/electroneum [https://perma.cc/G472-FXK5] (last visited Feb. 2, 2019).

417. Id.

418. Id.

419. Electroneum, CoinMarketCap, http://coinmarketcap.com/currencies/electroneum/historical-data/?start=20130428&end=20190124 [http://perma.cc/3HUS-4G52] (last visited Jan. 24, 2019) (reported as of Dec. 14, 2017).

420. Id.

421. Aeternity, ICOmarks, https://icomarks.com/ico/aeternity [https://perma.cc/SXQ6-CJAE] (last visited Jan. 24, 2019).

422. Id.

423. Id.

424. Aeternity, CoinMarketCap, https://coinmarketcap.com/currencies/aeternity/historical-data/?start=20130428&end=20190124 [https://perma.cc/K5AD-ZDLJ] (last visited Jan. 24, 2019) (reported as of Sept. 8, 2017).

425. Id.

Monetha	LTU[426]	$37.0[427]	8/31/17[428]	$61.1[429]	$4.2[430]
Basic Attention	USA[431]	$15.0[432]	5/31/17[433]	$171.0[434]	$156.9[435]
Stox	GIB[436]	$33.0[437]	8/4/17[438]	$36.0[439]	$0.6[440]
Civic	USA[441]	$33.0[442]	6/22/17[443]	$60.0[444]	$17.5[445]
Request Network	DEU[446]	$32.9[447]	10/17/17[448]	$38.7[449]	$15.4[450]

426. Monetha, ICOmarks, https://www.icomarks.com/ico/monetha [https://perma.cc/GG2J-G67Y] (last visited Feb. 2, 2019).

427. Id.

428. Id.

429. Monetha, CoinMarketCap, https://coinmarketcap.com/currencies/monetha/historical-data/?start=20130428&end=20190124 [https://perma.cc/PQ8E-QS9V] (last visited Jan. 24, 2019) (reported as of Sept. 6, 2017).

430. Id.

431. Basic Attention Token, ICOmarks, https://icomarks.com/ico/basic-attention [https://perma.cc/982X-8JZG] (last visited Jan. 24, 2019).

432. Id.

433. Id.

434. Basic Attention Token, CoinMarketCap, https://coinmarketcap.com/currencies/basic-attention-token/historical-data/?start=20130428&end=20190124 [https://perma.cc/P3JK-3W92] (last visited Jan. 24, 2019) (reported as of June 1, 2017).

435. Id.

436. Stox, ICOmarks, https://icomarks.com/ico/stox [https://perma.cc/2Q42-GJN3] (last visited Jan. 24, 2019).

437. Id.

438. Id.

439. Stox, CoinMarketCap, https://coinmarketcap.com/currencies/stox/historical-data/?start=20130428&end=20190124 [https://perma.cc/L3BU-AC8T] (last visited Jan. 24, 2019) (reported as of Aug. 5, 2017).

440. Id.

441. Civic, ICOmarks, https://icomarks.com/ico/civic [https://perma.cc/57KQ-HRFY] (last visited Jan. 24, 2019).

442. Id.

443. Id.

444. Civic, CoinMarketCap, https://coinmarketcap.com/currencies/civic/historical-data/?start=20130428&end=20190124 [https://perma.cc/K2GC-34W8] (last visited Jan. 24, 2019) (reported as of July 17, 2017).

445. Id.

446. Request Network, ICOmarks, https://icomarks.com/ico/request-network [https://perma.cc/CH84-KXJ5] (last visited Jan. 24, 2019).

447. Id.

448. Id.

449. Request Network, CoinMarketCap, https://coinmarketcap.com/currencies/request-network/historical-data/?start=20130428&end=20190124 [https://perma.cc/Z3KU-M55T] (last visited Jan. 24, 2019) (reported as of Oct. 20, 2017).

450. Id.

Grid+	USA[451]	$32.2[452]	11/12/17[453]	$35.8[454]	$1.8[455]
ChainLink	USA[456]	$32.0[457]	9/19/17[458]	$66.2[459]	$101.3[460]
Polybius	EST[461]	$31.0[462]	6/30/17[463]	$12.8[464]	$3.9[465]
Unikoin Gold	USA[466]	$28.6[467]	10/23/17[468]	$15.8[469]	$3.0[470]
DomRaider	FRA[471]	$45.0[472]	10/9/17[473]	$16.8[474]	$1.2[475]

451. Grid+, ICODrops, https://icodrops.com/grid/ [https://perma.cc/M6GT-LB2U] (last visited Jan. 24, 2019).

452. Id.

453. Id.

454. Grid+, CoinMarketCap, https://coinmarketcap.com/currencies/grid/historical-data/?start=20130428&end=20190124 [https://perma.cc/6UBQ-XUSG] (last visited Jan. 24, 2019) (reported as of Nov. 13, 2017).

455. Id.

456. ChainLink, ICODrops, https://icodrops.com/chainlink/ [https://perma.cc/CWZ2-EJZS] (last visited Jan. 24, 2019).

457. Id.

458. Id.

459. Chainlink, CoinMarketCap, https://coinmarketcap.com/currencies/chainlink/historical-data/?start=20130428&end=20190124 [https://perma.cc/97VG-FDA6] (last visited Jan. 24, 2019) (reported as of Sept. 20, 2017).

460. Id.

461. Polybius, ICOmarks, https://icomarks.com/ico/polybius [https://perma.cc/5NV3-U8LQ] (last visited Jan. 24, 2019).

462. Id.

463. Id.

464. Polybius, CoinMarketCap, https://coinmarketcap.com/currencies/polybius/historical-data/?start=20130428&end=20190124 [https://perma.cc/VA5C-XVV6] (last visited Jan. 24, 2019) (reported as of July 15, 2017).

465. Id.

466. Unikoin Gold, ICOmarks, https://icomarks.com/ico/unikrn [https://perma.cc/869H-YA4Z] (last visited Jan. 24, 2019).

467. Id.

468. Id.

469. Unikoin Gold, CoinMarketCap, https://coinmarketcap.com/currencies/unikoin-gold/historical-data/?start=20130428&end=20190124 [https://perma.cc/J8M7-4NJX] (last visited Jan. 24, 2019) (reported as of Nov. 21, 2017).

470. Id.

471. DomRaider, ICOmarks, https://icomarks.com/ico/domraider [https://perma.cc/5MH8-QHZK] (last visited Jan. 24, 2019).

472. Id.

473. Id.

474. DomRaider, CoinMarketCap, https://coinmarketcap.com/currencies/domraider/historical-data/?start=20130428&end=20190124 [https://perma.cc/R2LV-CACL] (last visited Jan. 24, 2019) (reported as of Nov. 6, 2017).

475. Id.

Blackmoon	CYP[476]	$30.0[477]	10/12/17[478]	$25.3[479]	$3.8[480]
Bankera	LTU[481]	$150.9[482]	2/27/18[483]	N/A[484]	N/A[485]
Agrello	EST[486]	$35.0[487]	8/17/17[488]	$34.5[489]	$3.3[490]
Storj	USA[491]	$30.0[492]	5/25/17[493]	$23.5[494]	$19.3[495]
Eidoo	CHE[496]	$28.0[497]	10/16/17[498]	$25.5[499]	$22.3[500]

476. Blackmoon, ICOmarks, https://icomarks.com/ico/blackmoon [https://perma.cc/Y6EX-L7DM] (last visited Jan. 24, 2019).

477. Id.

478. Id.

479. Blackmoon, CoinMarketCap, https://coinmarketcap.com/currencies/blackmoon/historical-data/?start=20130428&end=20190124 [https://perma.cc/5L3R-QQPN] (last visited Jan. 24, 2019) (reported as of Sept. 20, 2017).

480. Id.

481. Bankera, ICOmarks, https://icomarks.com/ico/bankera [https://perma.cc/4CQU-L6VF] (last visited Jan. 24, 2019).

482. Id.

483. Id.

484. No market capitalization data for Bankera were available from publicly available coin-focused websites.

485. See supra note 484.

486. Agrello, ICOmarks, https://icomarks.com/ico/agrello [https://perma.cc/M8QM-FEPB] (last visited Jan. 24, 2019).

487. Id.

488. Id.

489. Agrello, CoinMarketCap, https://coinmarketcap.com/currencies/agrello-delta/historical-data/?start=20130428&end=20190124 [https://perma.cc/DA72-2RW9] (last visited Jan. 24, 2019) (reported as of Sept. 9, 2017).

490. Id.

491. Storj, ICOmarks, https://icomarks.com/ico/storj [https://perma.cc/WK6J-W4ZR] (last visited Jan. 24, 2019).

492. Id.

493. Id.

494. Storj, CoinMarketCap, https://coinmarketcap.com/currencies/storj/historical-data/?start=20130428&end=20190124 [https://perma.cc/UX89-8YXN] (last visited Jan. 24, 2019) (reported as of July 2, 2017).

495. Id.

496. Eidoo, ICOmarks, https://icomarks.com/ico/eidoo [https://perma.cc/5JMZ-JBCQ] (last visited Jan. 24, 2019).

497. Id.

498. Id.

499. Eidoo, CoinMarketCap, https://coinmarketcap.com/currencies/eidoo/historical-data/?start=20130428&end=20190124 [https://perma.cc/D68K-KBQU] (last visited Jan. 24, 2019) (reported as of Oct. 17, 2017).

500. Id.

Monaco	CHE[501]	$26.7[502]	6/18/17[503]	$23.9[504]	$35.3[505]
Power Ledger	AUS[506]	$13.2[507]	10/6/17[508]	$76.6[509]	$32.0[510]
Everex	SGP[511]	$26.7[512]	8/31/17[513]	$31.5[514]	$4.4[515]
Decentraland	ARG[516]	$24.0[517]	8/8/17[518]	$18.7[519]	$47.7[520]
FunFair	GBR[521]	$20.0[522]	6/23/17[523]	$348.3[524]	$22.9[525]

501. Monaco, ICODrops, https://icodrops.com/monaco/ [https://perma.cc/JGG8-PRE9] (last visited Jan. 24, 2019).

502. Id.

503. Id.

504. Crypto.com, CoinMarketCap, https://coinmarketcap.com/currencies/crypto-com/historical-data/?start=20130428&end=20190124 [https://perma.cc/R2UG-JSG8] (last visited Jan. 24, 2019) (reported as of July 3, 2017).

505. Id.

506. Power Ledger, ICOmarks, https://icomarks.com/ico/power-ledger [https://perma.cc/F4E6-7TA5] (last visited Jan. 24, 2019).

507. Id.

508. Id.

509. Power Ledger, CoinMarketCap, https://coinmarketcap.com/currencies/power-ledger/historical-data/?start=20130428&end=20190124 [https://perma.cc/AXD8-UTEA] (last visited Jan. 24, 2019) (reported as of Nov. 6, 2017).

510. Id.

511. Everex, ICOmarks, https://icomarks.com/ico/everex [https://perma.cc/3BVJ-FW6P] (last visited Jan. 24, 2019).

512. Id.

513. Id.

514. Everex, CoinMarketCap, https://coinmarketcap.com/currencies/everex/historical-data/?start=20130428&end=20190203 [https://perma.cc/8GXU-H92P] (last visited Feb. 2, 2019) (reported as of Oct. 10, 2017).

515. Id.

516. Decentraland, ICOmarks, https://icomarks.com/ico/decentraland [https://perma.cc/8QLC-AVFC] (last visited Jan. 24, 2019).

517. Id.

518. Id.

519. Decentraland, CoinMarketCap, https://coinmarketcap.com/currencies/decentraland/historical-data/?start=20130428&end=20190203 [https://perma.cc/G6VA-S7DG] (last visited Feb. 2, 2019) (reported as of Sept. 28, 2017).

520. Id.

521. FunFair, ICOmarks, https://icomarks.com/ico/funfair [https://perma.cc/9NQ9-C6QL] (last visited Jan. 24, 2019).

522. Id.

523. Id.

524. FunFair, CoinMarketCap, https://coinmarketcap.com/currencies/funfair/historical-data/?start=20130428&end=20190203 [https://perma.cc/5CMJ-6FZA] (last visited Feb. 2, 2019) (reported as of July 2, 2017).

525. Id.

BitClave	USA[526]	$25.5[527]	11/29/17[528]	$81.7[529]	$0.3[530]
Tierion	USA[531]	$25.0[532]	7/28/17[533]	$81.6[534]	$5.0[535]
OmiseGo	SGP[536]	$25.0[537]	7/23/17[538]	$42.6[539]	$189.5[540]
Aragon	ESP[541]	$25.0[542]	5/17/17[543]	$36.9[544]	$11.2[545]
0x	USA[546]	$24.0[547]	9/15/17[548]	$134.6[549]	$163.9[550]

526. BitClave, ICOmarks, https://icomarks.com/ico/bitclave [https://perma.cc/7JVU-DC8N] (last visited Jan. 24, 2019).

527. Id.

528. Id.

529. BitClave, CoinMarketCap, https://coinmarketcap.com/currencies/bitclave/historical-data/?start=20130428&end=20190203 [https://perma.cc/KR7E-WABF] (last visited Feb. 2, 2019) (reported as of Jan. 16, 2018).

530. Id.

531. Tierion, ICOmarks, https://icomarks.com/ico/tierion [https://perma.cc/S44L-P449] (last visited Jan. 24, 2019).

532. Id.

533. Id.

534. Tierion, CoinMarketCap, https://coinmarketcap.com/currencies/tierion/historical-data/?start=20130428&end=20190203 [https://perma.cc/S34T-QHJZ] (last visited Feb. 2, 2019) (reported as of Aug. 27, 2017).

535. Id.

536. OmiseGo, ICOmarks, https://icomarks.com/ico/omisego [https://perma.cc/N7G3-YV8M] (last visited Jan. 24, 2019).

537. Id.

538. Id.

539. OmiseGo, CoinMarketCap, https://coinmarketcap.com/currencies/omisego/historical-data/?start=20130428&end=20190203 [https://perma.cc/QCU9-EH6B] (last visited Feb. 2, 2019) (reported as of July 15, 2017).

540. Id.

541. Aragon, ICOmarks, https://icomarks.com/ico/aragon [https://perma.cc/DB26-QH48] (last visited Jan. 24, 2019).

542. Id.

543. Id.

544. Aragon, CoinMarketCap, https://coinmarketcap.com/currencies/aragon/historical-data/?start=20130428&end=20190203 [https://perma.cc/4LRD-3NSK] (last visited Feb. 2, 2019) (reported as of May 19, 2017).

545. Id.

546. 0x, ICOmarks, https://icomarks.com/ico/0x [https://perma.cc/K6MJ-ZDCN] (last visited Jan. 24, 2019).

547. Id.

548. Id.

549. 0x, CoinMarketCap, https://coinmarketcap.com/currencies/0x/historical-data/?start=20130428&end=20190203 [https://perma.cc/9CZ8-KVJD] (last visited Feb. 2, 2019) (reported as of Aug. 16, 2017).

550. Id.

Enjin Coin	SGP[551]	$23.0[552]	10/31/17[553]	$18.7[554]	$28.6[555]
BLOCKv	USA[556]	$21.5[557]	10/25/17[558]	$31.6[559]	$7.2[560]
FinShi Capital	SGP[561]	$21.4[562]	10/6/17[563]	N/A[564]	N/A[565]
UTRUST	CHE[566]	$20.0[567]	11/20/17[568]	$68.1[569]	$10.0[570]
Target Coin	IND[571]	$20.7[572]	8/31/17[573]	$28.8[574]	$0.8[575]

551. Enjin Coin, ICOmarks, https://icomarks.com/ico/enjin-coin [https://perma.cc/UY3T-GJB4] (last visited Jan. 24, 2019).

552. Id.

553. Id.

554. Enjin Coin, CoinMarketCap, https://coinmarketcap.com/currencies/enjin-coin/historical-data/?start=20130428&end=20190203 [https://perma.cc/7DY8-XLH9] (last visited Feb. 2, 2019) (reported as of Nov. 15, 2017).

555. Id.

556. BLOCKv, ICOmarks, https://icomarks.com/ico/blockv [https://perma.cc/68GU-VQM4] (last visited Jan. 24, 2019).

557. Id.

558. Id.

559. BLOCKv, CoinMarketCap, https://coinmarketcap.com/currencies/blockv/historical-data/?start=20130428&end=20190203 [https://perma.cc/BCB8-XVY3] (last visited Feb. 2, 2019) (reported as of Dec. 7, 2017).

560. Id.

561. FinShi Capital, ICOmarks, https://icomarks.com/ico/finshi-capital [https://perma.cc/FT72-X3FL] (last visited Jan. 24, 2019).

562. Id.

563. Id.

564. No market capitalization data for FinShi Capital was available from publicly available coin-focused websites.

565. See supra note 564.

566. UTRUST, ICOmarks, https://icomarks.com/ico/utrust [https://perma.cc/5KVG-YVUT] (last visited Jan. 24, 2019).

567. Id.

568. Id.

569. UTRUST, CoinMarketCap, https://coinmarketcap.com/currencies/utrust/historical-data/?start=20130428&end=20190203 [https://perma.cc/SWZ8-Y629] (last visited Feb. 2, 2019) (reported as of Dec. 29, 2017).

570. Id.

571. Target Coin, ICOmarks, https://icomarks.com/ico/target-coin [https://perma.cc/QGL2-C2R2] (last visited Jan. 24, 2019).

572. Id.

573. Id.

574. Target Coin, CoinMarketCap, https://coinmarketcap.com/currencies/target-coin/historical-data/?start=20130428&end=20190203 [https://perma.cc/UZ72-G6DZ] (last visited Feb. 2, 2019) (reported as of Oct. 7, 2017).

575. Id.

ATB Coin	USA[576]	$20.4[577]	9/1/17[578]	$35.2[579]	$0.4[580]
Giga Watt	USA[581]	$15.0[582]	7/31/17[583]	$4.3[584]	$1.6[585]
Total	*N/A*	*$2,584.0*	*N/A*	*$6,969.7*	*$5,335.1*

576. ATB Coin, ICOmarks, https://icomarks.com/ico/atb-coin [https://perma.cc/L7DV-MNDS] (last visited Jan. 24, 2019).

577. Id.

578. Id.

579. ATBCoin, CoinMarketCap, https://coinmarketcap.com/currencies/atbcoin/historical-data/?start=20130428&end=20190203 [https://perma.cc/GV7E-D6MB] (last visited Feb. 18, 2019) (reported as of Oct. 7, 2017).

580. Id.

581. Giga Watt, ICOmarks, https://icomarks.com/ico/giga-watt [https://perma.cc/H4CW-CWNF] (last visited Jan. 24, 2019).

582. Id.

583. Id.

584. Giga Watt Token, CoinMarketCap, https://coinmarketcap.com/currencies/giga-watt-token/historical-data/?start=20130801&end=20190125 [https://perma.cc/AXD8-UTEA] (last visited Jan. 24, 2019) (reported as of Sept. 2, 2017).

585. Id.

APPENDIX B: SUMMARY OF CODE/CONTRACT AUDIT

ICOName	**Scarcity Claimed (Y/N)[586] Scarcity Coded (Y/N)[587]**	**Burning Claimed (Y/N)[588] Burning Coded (Y/N)[589]**	**Vesting Claimed (Y/N)[590] Vesting Coded (Y/N)[591]**	**Modification Disclosed (Y/N)[592] Modification Coded (Y/N)[593]**
Filecoin[594]	N/A	N/A	N/A	N/A
Tezos[595]	ScarcityNN	BurningYN	VestingYN	ModificationNN
EOS Stage 1[596]	ScarcityNN	BurningNN	VestingYN	ModificationNN
Paragon[597]	ScarcityYY	BurningYY	VestingNN	ModificationNN
Bancor[598]	ScarcityYN	BurningYY	VestingYN	ModificationNN

586. For individualized details related to claims of token scarcity for each ICO, see generally Appendix C, supra note 69.

587. All claims are evaluated individually based on each ICO's smart contract. Individual contracts for each ICO are cited at infra notes 594–645.

588. For individualized details related to claims of token burning for each ICO, see generally Appendix C, supra note 69.

589. All claims are evaluated individually based on each ICO's smart contract. Individual contracts for each ICO are cited at infra notes 594–645.

590. For individualized details related to claims of token vesting for each ICO, see generally Appendix C, supra note 69.

591. All claims are evaluated individually based on each ICO's smart contract. Individual contracts for each ICO are cited at infra notes 594–645.

592. For individualized details related to claims of token modifications for each ICO, see generally Appendix C, supra note 69.

593. All claims are evaluated individually based on each ICO's smart contract. Individual contracts for each ICO are cited at infra notes 594–645.

594. Filecoin's ICO buyers received traditional investment agreements that promise delivery of cryptoassets in the future. See Bennett Garner, What Is Filecoin? Beginner's Guide to the Largest-Ever ICO, CoinCentral (Feb. 20, 2018), https://coincentral.com/filecoin-beginners-guide-largest-ever-ico/ [https://perma.cc/PJ52-J335]; see also Appendix C, supra note 69. To date, Filecoin has not made any smart contract code publicly available for audit on Etherscan. See Email from Marvin Ammori, Gen. Counsel of Protocol Labs, to David Hoffman, Professor of Law, Univ. of Pa. Law Sch. (Aug. 2, 2018) (on file with the *Columbia Law Review*) (confirming that the organization was not affiliated with any tokens labeled "Filecoin" available on Etherscan).

595. Tezos ran simultaneous capital raising efforts on both the Bitcoin and Ethereum networks. Following the development of the independent Tezos blockchain, contributors were to be manually allocated "Tezzies" (the associated coin) on the new chain, in proportion to their contributions. The "ICO" contract on the Ethereum blockchain provided no such guarantee. See Steven O'Neal, The History of Tezos: The Infamous ICO Trying to Rebound Amidst Lawsuits and Disputes, CoinTelegraph (July 5, 2018), https://cointelegraph.com/news/the-history-of-tezos-the-infamous-ico-trying-to-rebound-amidst-lawsuits-and-disputes [https://perma.cc/F88J-5BDW].

596. EOSIO, Eos-Token-distribution, Github (July 5, 2017), https://github.com/EOSIO/eos-token-distribution/blob/master/src/eos_sale.sol [https://perma.cc/8TXF-XTEH].

597. Paragon (PRG), supra note 178.

598. Bancor (BNT), Contract Code, Etherscan, https://etherscan.io/address/0x1f573d6fb3f13d689ff844b4ce37794d79a7ff1c#code [https://perma.cc/JD5L-U6CL] (last visited Feb. 16, 2019).

Kin[599]	ScarcityYY	BurningNN	VestingYY	ModificationNN
Status[600]	ScarcityYN	BurningYY	VestingYY	ModificationYY
Tron[601]	ScarcityYY	BurningNN	VestingYN	ModificationNN
TenX[602]	ScarcityYN	BurningNN	VestingYN	ModificationNN
MobileGo[603]	ScarcityYY	BurningYY	VestingNN	ModificationNN
KyberNetwork[604]	ScarcityYY	BurningYY	VestingYN	ModificationNN
MCAP[605]	ScarcityYY	BurningNN	VestingNN	ModificationNN
Loopring[606]	ScarcityYY	BurningNN	VestingNN	ModificationNN
Enigma Catalyst[607]	ScarcityYY	BurningYN	VestingYN	ModificationNN
ICON[608]	ScarcityNY	BurningNY	VestingYN	ModificationNN
PeerBanks[609]	ScarcityYY	BurningNN	VestingNN	ModificationNN
Electroneum[610]	ScarcityYN	BurningNN	VestingYN	ModificationNN
Aeternity[611]	ScarcityYY	BurningYN	VestingYN	ModificationNN

599. Kin (KIN), supra note 154.

600. StatusNetwork (SNT), supra note 183.

601. Tronix (TRX), Contract Code, Etherscan, https://etherscan.io/address/0xf230b790e05390fc8295f4d3f60332c93bed42e2#code [https://perma.cc/ZF45-QSTX] (last visited Feb. 16, 2019).

602. TenXPay (PAY), Contract Code, Etherscan, https://etherscan.io/address/0xB97048628DB6B661D4C2aA833e95Dbe1A905B280#code [https://perma.cc/87RH-XDAX] (last visited Feb. 16, 2019).

603. MobileGo (MGO), Contract Code, Etherscan, https://etherscan.io/address/0x40395044Ac3c0C57051906dA938B54BD6557F212#code [https://perma.cc/2WFL-QZ9W] (last visited Feb. 16, 2019).

604. KyberNetwork (KNC), Contract Code, Etherscan, https://etherscan.io/address/0xdd974d5c2e2928dea5f71b9825b8b646686bd200#code [https://perma.cc/J5T9-83T7] (last visited Feb. 16, 2019).

605. MCAP (MCAP), Contract Code, Etherscan, https://etherscan.io/address/0x93e682107d1e9defb0b5ee701c71707a4b2e46bc#code [https://perma.cc/7MJN-GAJR] (last visited Feb. 16, 2019).

606. Loopring (LRC), Contract Code, Etherscan, https://etherscan.io/address/0xef68e7c694f40c8202821edf525de3782458639f#code [https://perma.cc/L8K8-3Z9Z] (last visited Feb. 16, 2019).

607. Enigma (ENG), Contract Code, Etherscan, https://etherscan.io/address/0xf0ee6b27b759c9893ce4f094b49ad28fd15a23e4#code [https://perma.cc/P622-PA3Q] (last visited Feb. 16, 2019).

608. ICON (ICX), Contract Code, Etherscan, https://etherscan.io/address/0xb5a5f22694352c15b00323844ad545abb2b11028#code [https://perma.cc/6Z4P-PLEU] (last visited Feb. 16, 2019).

609. PEERBANKS (IRA), Contract Code, Etherscan, https://etherscan.io/address/0xcb73cef85b5d50a23a580919e72818fd2264c0f5#code [https://perma.cc/RXU7-37BD] (last visited Feb. 16, 2019).

610. This ICO was performed entirely off chain, prior to the launch of the Electroneum network. As a result, automated enforcement of the promises made in the whitepaper was not available.

611. Aeternity (AE), Contract Code, Etherscan, https://etherscan.io/address/0x5ca9a71b1d01849c0a95490cc00559717fcf0d1d#code [https://perma.cc/K46G-E6H5] (last visited Feb. 16, 2019).

Monetha[612]	ScarcityYY	BurningYY	VestingYY	ModificationNN
Basic Attention Token[613]	ScarcityYY	BurningNN	VestingYY[614]	ModificationNN
Stox[615]	ScarcityYY	BurningNY	VestingYY	ModificationNY
Civic[616]	ScarcityYY	BurningNN	VestingYN	ModificationNY
Request Network[617]	ScarcityYY	BurningYY	VestingNY	ModificationNN
Grid+ [618]	ScarcityYY	BurningYN	VestingYY	ModificationNN
ChainLink[619]	ScarcityYY	BurningNN	VestingNN	ModificationNN
Polybius[620]	Unauditable	Unauditable	Unauditable	ModificationYY
Unikoin Gold[621]	ScarcityYY	BurningNN	VestingNN	ModificationNN
DomRaider[622]	ScarcityYY	BurningNN	VestingYY	ModificationNN

612. Monetha (MTH), Contract Code, Etherscan, https://etherscan.io/address/0xaf4dce16da2877f8c9e00544c93b62ac40631f16#code [https://perma.cc/35DX-3GUY] (last visited Feb. 16, 2019).

613. Basic Attention Token (BAT), Contract Code, Etherscan, https://etherscan.io/address/0x0d8775f648430679a709e98d2b0cb6250d2887ef#code [https://perma.cc/26YV-YR3F] (last visited Feb. 16, 2019).

614. BAT implements vesting via a secondary smart contract, to which tokens were transferred before the ICO. See BATSafe, Contract Code, Etherscan, https://etherscan.io/address/0x67fa2c06c9c6d4332f330e14a66bdf1873ef3d2b#code [https://perma.cc/A2GE-LWWN] (last visited Jan. 25, 2019).

615. Stox (STX), Contract Code, Etherscan, https://etherscan.io/address/0x006bea43baa3f7a6f765f14f10a1a1b08334ef45#code [https://perma.cc/6Z6V-U94T] (last visited Feb. 16, 2019).

616. Civic (CVC), Contract Code, Etherscan, https://etherscan.io/address/0x41e5560054824ea6b0732e656e3ad64e20e94e45#code [https://perma.cc/G6PU-2TFA] (last visited Feb. 16, 2019).

617. Request (REQ), Contract Code, Etherscan, https://etherscan.io/address/0x8f8221afbb33998d8584a2b05749ba73c37a938a#code [https://perma.cc/G22E-FJ9N] (last visited Feb. 16, 2019).

618. Sale, Contract Code, Etherscan, https://etherscan.io/address/0x94dc1cf66c8fd62ef3bd7da53f47423862839823#code [https://perma.cc/8BJT-93F8] (last visited Feb. 16, 2019).

619. ChainLink Token (LINK), Contract Code, Etherscan, https://etherscan.io/address/0x514910771af9ca656af840dff83e8264ecf986ca#code [https://perma.cc/J367-VV4R] (last visited Feb. 16, 2019).

620. This ICO constitutes a "proxy contract": a primary smart contract with which users interact and a secondary smart contract whose code is incorporated by reference. The primary contract for this ICO is written in Solidity and stores the modifiable reference along with code controlling how the reference may be changed, thus modifying the overall functionality. The secondary smart contract is available on Etherscan but only in bytecode format. As all functionality other than modification is delegated to the secondary bytecode contract, we were unable to audit the scarcity, burning, and vesting whitepaper claims. See Polybius (PLBT), supra note 205.

621. Unikoin Gold (UKG), Contract Code, Etherscan, https://etherscan.io/address/0x24692791bc444c5cd0b81e3cbcaba4b04acd1f3b#code [https://perma.cc/KWA3-4DT7] (last visited Feb. 16, 2019).

622. DomRaiderToken (DRT), Contract, Etherscan, https://etherscan.io/address/0x9af4f26941677c706cfecf6d3379ff01bb85d5ab#code [https://perma.cc/B9DL-897Y] (last visited Feb. 16, 2019).

Blackmoon Crypto[623]	Unauditable	Unauditable	Unauditable	ModificationNY
Bankera[624]	ScarcityYN	BurningNN	VestingYN	ModificationNN
Agrello[625]	ScarcityYY	BurningNN	VestingYN	ModificationNN
Storj[626]	ScarcityYY	BurningYY	VestingYN[627]	ModificationNY
Eidoo[628]	ScarcityYN	BurningYY	VestingYY	ModificationNN
Monaco[629]	ScarcityYN	BurningYN	VestingYN	ModificationNY
Power Ledger[630]	ScarcityYY	BurningNN	VestingYN	ModificationNN
Everex[631]	ScarcityYY	BurningNN	VestingYN	ModificationNN
Decentraland[632]	ScarcityNN	BurningYY	VestingYN	ModificationNN
FunFair[633]	ScarcityYN	BurningYY	VestingYN	ModificationYY
Bitclave[634]	ScarcityYY	BurningYN	VestingYN	ModificationNY

623. This ICO constitutes a "proxy contract." For a detailed description of what constitutes a proxy contract, see supra note 620. As a result, for this ICO our audit was limited solely to claims related to Modification. See Blackmoon Crypto Token (BMC), supra note 200.

624. Banker Token (BNK), Contract Code, Etherscan, https://etherscan.io/address/0xc80c5e40220172b36adee2c951f26f2a577810c5#code [https://perma.cc/3YCM-JMXE] (last visited Feb. 16, 2019).

625. Delta (DLT), Contract Code, Etherscan, https://etherscan.io/address/0x07e3c70653548b04f0a75970c1f81b4cbbfb606f#code [https://perma.cc/S5DZ-J2XR] (last visited Feb. 16, 2019).

626. Storj (STORJ), Contract Code, Etherscan, https://etherscan.io/address/0xb64ef51c888972c908cfacf59b47c1afbc0ab8ac#code [https://perma.cc/ZF7X-Y69P] (last visited Feb. 16, 2019).

627. Storj is a hard case. It built a token-based vesting regime outside of its ICO smart contract. For the vesting contract and associated transaction log, see TokenVault, Contract Overview, Etherscan, https://etherscan.io/address/0x34f34f58c50ef059b766065dbb24f7cf885e6463 [https://perma.cc/FE7X-DH8P] (last visited Mar. 22, 2019). While we believe that the project team manually transferred tokens for lockup into that second contract, this was not an automatic process. Nor (as with BAT, supra note 614) was it completed manually in advance of the ICO.

628. Eidoo (EDO), Contract Code, Etherscan, https://etherscan.io/address/0xced4e93198734ddaff8492d525bd258d49eb388e#code [https://perma.cc/6MFT-LRZC] (last visited Feb. 16, 2019).

629. Monaco (MCO), supra note 206.

630. Power Ledger (POWR), Contract Code, Etherscan, https://etherscan.io/address/0x595832f8fc6bf59c85c527fec3740a1b7a361269#code [https://perma.cc/32AB-WBVN] (last visited Feb. 22, 2019).

631. Everex (EVX), Contract Code, Etherscan, https://etherscan.io/address/0xf3db5fa2c66b7af3eb0c0b782510816cbe4813b8#code [https://perma.cc/ZP4X-EL5G] (last visited Feb. 16, 2019).

632. Decentraland (MANA), Contract Code, Etherscan, https://etherscan.io/address/0x0f5d2fb29fb7d3cfee444a200298f468908cc942#code [https://perma.cc/XK5P-PMNL] (last visited Feb. 16, 2019).

633. FunFair (FUN), Contract Code, Etherscan, https://etherscan.io/address/0x419d0d8bdd9af5e606ae2232ed285aff190e711b#code [https://perma.cc/KYH7-NFS8] (last visited Feb. 16, 2019).

634. BitClave (CAT), Contract Code, Etherscan, https://etherscan.io/address/0x1234567461d3f8db7496581774bd869c83d51c93#code [https://perma.cc/D6BP-3Q6H] (last visited Feb. 16, 2019).

Tierion[635]	ScarcityYY	BurningNN	VestingYN	ModificationNN
OmiseGo[636]	ScarcityYN	BurningYN	VestingYN	ModificationYN
Aragon[637]	ScarcityNN	BurningNY	VestingYY	ModificationYY
0x[638]	ScarcityYY	BurningNN	VestingYN	ModificationNN
Enjin[639]	ScarcityYY	BurningNN	VestingYY	ModificationNN
BlockV[640]	ScarcityYY	BurningNN	VestingYY	ModificationNY
FinShi Capital[641]	Unauditable	Unauditable	Unauditable	ModificationNY
UTRUST[642]	ScarcityYY	BurningYY	VestingYN	ModificationYN
Target Coin[643]	ScarcityYN	BurningNN	VestingNN	ModificationNN
ATB Coin[644]	Unauditable	Unauditable	Unauditable	Unauditable
Giga Watt[645]	ScarcityYN	BurningNN	VestingYN	ModificationYN

635. Tierion Network Token (TNT), Contract Code, Etherscan, https://etherscan.io/address/0x08f5a9235b08173b7569f83645d2c7fb55e8ccd8#code [https://perma.cc/U2VN-EX32] (last visited Feb. 16, 2019).

636. OmiseGO (OMG), Contract Code, Etherscan, https://etherscan.io/address/0xd26114cd6EE289AccF82350c8d8487fedB8A0C07#code [https://perma.cc/36TP-ERFH] (last visited Feb. 16, 2019).

637. Aragon (ANT), Contract Code, Etherscan, https://etherscan.io/address/0x960b236A07cf122663c4303350609A66A7B288C0#code [https://perma.cc/J37D-DBVQ] (last visited Feb. 16, 2019).

638. ZRX (ZRX), Contract Code, Etherscan, https://etherscan.io/address/0xe41d2489571d322189246dafa5ebde1f4699f498#code [https://perma.cc/42Z2-R23M] (last visited Feb. 16, 2019).

639. EnjinCoin (ENJ), Contract Code, Etherscan, https://etherscan.io/address/0xf629cbd94d3791c9250152bd8dfbdf380e2a3b9c#code [https://perma.cc/ZCF7-UKVK] (last visited Feb. 16, 2019).

640. BLOCKv (VEE), Contract Code, Etherscan, https://etherscan.io/address/|0x340d2bde5eb28c1eed91b2f790723e3b160613b7#code [https://perma.cc/KB8N-X33B] (last visited Feb. 16, 2019).

641. This ICO constitutes a "proxy contract." For a detailed description of what constitutes a proxy contract, see supra note 620. As a result, for this ICO our audit was limited solely to claims related to Modification. See FinShi Capital Tokens (FINS) Contract Code, Etherscan, https://etherscan.io/address/0x4805e471dd86dc0e3cbe44305391e37e491b579e#code [https://perma.cc/HN3V-6R79] (last visited Feb. 16, 2019).

642. UTRUST (UTK), Contract Code, Etherscan, https://etherscan.io/address/0x70a72833d6bf7f508c8224ce59ea1ef3d0ea3a38#code [https://perma.cc/NHL2-H3F5] (last visited Feb. 16, 2019).

643. Target Coin (TGT), Contract Code, Etherscan, https://etherscan.io/address/0xac3da587eac229c9896d919abc235ca4fd7f72c1#code [https://perma.cc/QD9D-T8SC] (last visited Feb. 16, 2019).

644. ATB Coin received ICO contributions through a wallet address rather than a smart contract address. The Ethereum network therefore provides no restrictions on the use of the funds by the owners of the address. Contributors were to later receive tokens through a manual process following the development of the ATB network. 0x13CA7Bb198aA6f8dbEe853742501B691497DE333, Overview, Etherscan, https://etherscan.io/address/0x13ca7bb198aa6f8dbee853742501b691497de333 (on file with the *Columbia Law Review*) (last visited Mar. 23, 2019).

645. WTT (WTT), Contract Code, Etherscan, https://etherscan.io/address/0x84119cb33e8f590d75c2d6ea4e6b0741a7494eda#code [https://perma.cc/FQE8-ZU5N] (last visited Feb. 16, 2019).