

COIN-OPERATED CAPITALISM

Shaanan Cohney, David Hoffman,
Jeremy Sklaroff and 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, where 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, “white papers,” 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 previously undisclosed code permitting modification of the entities’ governing structures.

† Author order is alphabetical. Cohney is a fifth-year doctoral student in computer and information science at the University of Pennsylvania, where Hoffman is a Professor of Law, Sklaroff received a JD/MBA in 2018, and Wishnick is a fellow at the Law School’s Center for Technology, Innovation and Competition. We thank Andrew Baker, Tom Baker, Robert Bartlett, Bill Bratton, Chris Brummer, Tony Casey, Peter Conti-Brown, Jill Fisch, Gabe Kapchuk, Joshua Mitts, Mark Nevitt, Ori Oren, Max Raskin, Usha Rodrigues, Alec Webley, Kevin Werbach, 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 Workshop, 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.

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

¹ See, e.g., Chance Barnett, Trends Show Crowdfunding to Surpass VC After 2016, Medium.com (Jul. 22, 2016) <https://medium.com/startup-grind/trends-show-crowdfunding-to-surpass-vc-in-2016-65df924d8a82> [perma] (“[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, (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.

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” 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., to 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

⁴ Here, as elsewhere, this Article make 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 194.

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--II.B.

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. 1997), <https://journals.uic.edu/ojs/index.php/fm/article/view/548/469> [<https://perma.cc/KKT6-9PHC>].

⁷ 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/86X7-4H2N>] (last visited Jan. 28, 2019) (“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.”).

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 when ICOs entered popular consciousness¹¹—453 ICOs raised an estimated \$6.58 billion.¹² By July 1, 2018, an

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 approximately 20% of ICOs examined by the authors have red flags, including plagiarism in their white papers, 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://papers.ssrn.com/sol3/papers.cfm?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, *Dealbook: Easiest Path of 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). Popper, an excellent observer of this market at its inception, wrote generally on bitcoin phenomenon before it had reached a general audience. See Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (2015).

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/#5c0836f01183> [<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 273. Solely to ease exposition, this Article will generally use market values (in US dollars) reported by widely used coin-data sites.

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

Fourteen billion dollars raised over eighteen months is not chump-change, but it is \$2 billion less than what Facebook raised in one day with its 2012 IPO.¹⁵ Though you 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

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>] ("The ICO market is dead -- over.")

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, e.g., Usha Rodrigues, Law and the Blockchain, 104 *Iowa L. Rev.* 679 (2018); Kevin Werbach, Trust but Verify: Why the Blockchain Needs the Law, 33 *Berkeley Tech. L.J.* 487 (2018); Iris M. Barsan, Legal Challenges of Initial Coin Offerings, 3 *Revue Trimestrielle de Droit Financier* 54 (2017); Dirk A. Zetsche, Ross P. Buckley, Douglas W. Arner, & Linus Fohr, 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://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298 (on file with the Columbia Law Review) (noting severe disclosure failures in a global and rapidly growing market).

world is simple: how are 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

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 the Matter of Coinalpha Advisors LLC*, Respondent, 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. Dept. of Regulatory Agencies, *Two Companies Promoting Cryptocurrencies Under Scrutiny by Colorado Securities Commissioner* (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 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 cease-and-desist orders entered against the Airfox and Paragon ICO teams for sales of unregistered securities); Press Release, SEC, *SEC Charges EtherDelta Founder with Operating an Unregistered Exchange* (Nov. 8, 2018), <https://www.sec.gov/news/press-release/2018-258>

technologists admit that ICOs as a form of fundraising suffer credibility problems, as many projects have still not delivered on 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. Law'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

[<https://perma.cc/3ZU9-X747>] (discussing charges against the operator of a cryptoasset exchange that facilitate ICO token sales); 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 and the Democratization of Public Capital Markets 97 (Cardozo Leg. Stud. Res. Paper No. 527, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104 (on file with the Columbia Law Review) (discussing risk of fraud and abuse).

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.").

through computer code, rather than through legalistic means. This technological capacity is central to the ideological and practical case advanced by the entrepreneurs who engage in ICOs. They speak of automated, “[d]ynamic [c]eiling[s]” for cryptoasset supply²¹; of placing founders’ cryptoasset allocations in “time-locked smart contracts” to align incentives for productivity²²; 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 a substitute and complement for old-fashioned legal governance in financial contracting.

But “potential” does not mean “reality,” and our 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. We establish actual functionality by examining the 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

²¹ Status, The Status Network: A Strategy Towards Mass Adoption of Ethereum 28 (June 15, 2017), <https://status.im/whitepaper.pdf> [<https://perma.cc/Z233-EPQT>].

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

²³ See Protocol Labs, Filecoin: A Decentralized Storage Network 8 (July 19, 2017), <https://filecoin.io/filecoin.pdf> [<https://perma.cc/UL5G-CATU>].

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 Felippi & 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).

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 take-home 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

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 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 Res. 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).

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 pre-mortem on the current market's pathologies—this Part presents an operational account of ICO components and mechanics. Readers familiar with this topic could easily skim ahead to Part II.

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. In exchange for payment of a price (in dollars) set by investment bankers through careful underwriting, the team would part with shares of their 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 employees and suppliers in the same, and then distribute the leftovers to its shareholders.

The new world of coin-based finance looks very 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 they promise will be the only way to buy sodas from their (yet to be deployed) vending machines.²⁷ They 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 pay 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, 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 (roughly) reflect the net present value of the legal rights to the company's expected future cash flows,³⁰ crypto-token pricing should (roughly) reflect an equilibrium between token

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 Stud. Res. Paper Series, Res. 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* (3rd ed. 2012).

demand (driven by the present value of expected future use and exchange options within the token's native ecosystem) and token supply (driven by the token's monetary policy).³¹

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. No Wall Street

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* (2017) (suggesting cryptoasset valuation models); Catalini & Gans, *supra* note 26, at 3--5; Aswath Damodaran, *The Bitcoin Boom: Asset, Currency, Commodity, or Collectible?*, *Musings on Markets* (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 driven by Twitter followers and activity); Bourveau et al., *supra* note 26 (EP); Jongsub Lee, Tao Li, & Donghwa Shin, *The Wisdom of Crowds and Information Cascades in FinTech: Evidence From Initial Coin Offers* (Sept. 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).

investment bank has backed an ICO.³² Indeed, the absence of ICO-specific regulation and intermediaries is seen to be a feature, not a bug, by many enthusiasts.³³

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 by laws, regulations, contracts, and social norms.³⁴ ICO transactions augment, and perhaps replace, those mediators by embedding controls within the smart contracts through which rules function.³⁵ At the same time, they also create new roles for lawyers and legal-ish personnel.

The Colacoin clearly would be far more experimental a way to raise capital for the underlying soda company than through the sale of debt or equity.³⁶ 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.

³² 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)

³³ 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>] (“What else doesn’t matter to most crypto traders: 1. Licenses and regulatory approval.”).

³⁴ Though market fundamentalists might occasionally forget this, it is essential to any understanding of the contemporary economy. See, e.g., Katherina Pistor, *A Legal Theory of Finance*, 41 *J. Comp. Econ.* 315 (2013); David Singh Grewal, *Laws of Capitalism*, 128 *Harv. L. Rev.* 626 (2014) (reviewing Thomas Piketty, *Capital in the Twenty-First Century* (2014)).

³⁵ 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 (2006).

³⁶ 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).

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 capable of being transmitted. 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).³⁷ 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 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.³⁸

Cryptoasset history begins with Bitcoin currency and the Bitcoin ledger (also known as a “blockchain”).³⁹ Prior to their advent, money was either held in physical form (e.g., coins, paper notes), or on the ledger of a centralized intermediary (e.g., bank deposits, PayPal balances).⁴⁰ Bitcoin is the first significant digital currency system that needs no centralized intermediary to maintain proper books.⁴¹ The key to the ledger’s design—and that

³⁷ 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).

³⁸ 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.

³⁹ On the prehistory and history of Bitcoin, see Popper, *supra* note 10; 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>].

⁴⁰ See Morgan Ricks, The Money Problem: Rethinking Financial Regulation 58 (2016) (distinguishing between certificated and uncertificated forms of money).

⁴¹ See generally Kevin Werbach, Blockchain and the New Architecture of Trust (2018); Primavera De Filippi & Aaron Wright, Blockchain and the Law: The

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.⁴² These computers are called “nodes.”⁴³ 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.⁴⁴ 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.⁴⁵

The shift towards 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.⁴⁶ 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.⁴⁷ As a result, the value of ether depends significantly on the supply of, and demand for, computational power active on the Ethereum system. One of the key reasons for Ethereum’s popularity is its support for snippets of computer code

Rule of Code 61--71 (2018).

⁴² See Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller & Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies* 27--50 (2016); Böhme et al., *supra* note 37, at 216.

⁴³ Narayanan et al., *supra* note 42, at 7-10.

⁴⁴ See Werbach, *supra* note 16, at 512--13.

⁴⁵ 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, *supra* note 10. 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. of the ACM*, July 2018, at 95.

⁴⁶ See Werbach & Cornell, *supra* note 24, at 333--35; Rohr & Wright, *supra* note 18, at 19.

⁴⁷ Ethereum Whitepaper: A Next Generation Smart Contract & 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.*

that interact with the ledger known as smart contracts.⁴⁸ One can think of smart contracts as a pre-written 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.⁴⁹

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.⁵⁰ These inputs might include basic information about where to send ether, and also more complex information, like data from a weather vane.⁵¹ Ether plays roles as 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

⁴⁸ See generally Werbach & Cornell, *supra* note 24; 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); Jeremy M. Sklaroff, Comment, Smart Contracts and the Cost of Inflexibility, 166 *U. Penn. L. Rev.* 263 (2017).

⁴⁹ In most ways, calling these code snippets “contracts” is quite misleading, but we are stuck with the dominant terminology. For careful discussions, see J.G. Allen, *Wrapped and Stacked: “Smart Contracts” and the Interaction of Natural and Formal Language*, 14 *Euro. Rev. Contract L.* 307 (2018); James Grimmelmann, *All Smart Contracts Are Ambiguous*, *J. L. & Innov.* __ (forthcoming 2019), <https://ssrn.com/abstract=3315703> (on file with the Columbia Law Review).

⁵⁰ It also served as inspiration for Nick Szabo’s initial coinage of the smart-contract idea. See *supra* note 6 and accompanying text.

⁵¹ 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*, *Proc. 2016 ACM Conf. on Comp. & Comms. Sec. 1*; Houman Shadab, *What Smart Contracts Need to Learn*, *Lawbitrage* (Sept. 4, 2014), <http://lawbitrage.typepad.com/blog/2014/09/smart-contracts.html> [<https://perma.cc/H8AD-QAG9>].

insurance,⁵² escrow,⁵³ or even something akin to corporate formation.⁵⁴

To build increasingly complex and interoperating mechanisms within Ethereum, its community has begun developing standards---“fill in the blank” templates that perform agreed-on functions. One of those—standard “ERC-20”⁵⁵—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 Interface⁵⁶

⁵² 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).

⁵³ 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>].

⁵⁴ 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, *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.”)..

⁵⁵ 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.

⁵⁶ 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 55 and accompanying text.

```

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.

C. ICOs Hit the Bigtime

In 2014 Ethereum raised real money by selling ether to the public.⁵⁷ The next major ICO was Augur, in October 2015.⁵⁸ The market grew slowly until 2017, when it hit the gas.

⁵⁷ 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.

⁵⁸ 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 Ethereum in September 2014 and Augur in October

FIGURE 2: Number of ICOs by Month⁵⁹FIGURE 3: Total Raised in the ICO Market, By Month⁶⁰

As the ICO market exploded (and then subsided in the back half of 2018), so too did regulatory interest in its activities. Such scrutiny is no surprise: ICOs, like many Internet-based phenomena before them, intentionally take place at the regulatory perimeter.⁶¹ They exploit a basic tension between the

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].

⁵⁹ Data collected from www.coinschedule.com/stats.html and exclude the DAO

⁶⁰ Data collected from www.coinschedule.com/stats.html and exclude the DAO. The spike in March 2018 represents when the EOS raise was realized in the dataset, though it occurred continuously before.

⁶¹ 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

cross-jurisdictional and pseudonymous aspects of cryptocurrency transactions on the one hand and the objectives of regulators on the other.⁶² The question of just 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.⁶³ 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.⁶⁴ As of 2018, no similarly clear regime was in place for ICOs.⁶⁵ In lieu of the heavily-lawyered products of IPO documentation, the ICO

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 90s and continuing to the present, have recognized “that the Internet might provide profitable opportunities at the edges of the legal system”).

⁶² See, e.g., Sean Foley, Jonathan R. Karlsen, & Talis J. Putnins, Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?, 33 Rev. Fin. Stud. (forthcoming 2019), <https://ssrn.com/abstract=3102645> (on file with the Columbia Law Review) (finding that approximately one half of bitcoin transactions are associated with illicit activity). 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 Legis. Aff., U.S. Dep’t of Treas., to the Hon. Ron Wyden, Ranking Member, U.S. Senate Comm. on Fin. (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”).

⁶³ See What We Do, SEC, <https://www.sec.gov/Article/whatwedo.html>, [<https://perma.cc/75DL-EUXT>] (last visited Jan. 27, 2019).

⁶⁴ See id.

⁶⁵ In fact, the SEC only recently came out with guidance related to ICOs. **OPEN TO CITE GUIDANCE ONCE ISSUED.**

market coalesced on a less formal document known as a “white paper.”⁶⁶

Like governmental and non-profit white papers that seek to exemplify authoritative subject-mastery while gesturing towards collaborative openness, cryptoasset white papers are public documents that describe promoters’ plans for development and solicit community involvement.⁶⁷ Authoritative copies are typically available in PDF form on promoters’ websites and provided through listing services like coinschedule.com.⁶⁸ This makes white papers a transparent form of investor information, but obviates the need for outside vetting before they go live.

The legal status of white papers (and accompanying tweets, Medium posts, Reddit comments, and social media buzz) is unclear at best. Sometimes, white papers refer to—and embed—contractual terms and conditions of sale.⁶⁹ 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’s promised and what’s merely aspired-to.⁷⁰ 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 trade on hundreds of upstart markets, sometimes under light-to-nonexistent regulation.⁷¹ They are located in diverse jurisdictions and have

⁶⁶ See Barsan, *supra* note 16, at 54.

⁶⁷ Appendix [XX online]

⁶⁸ See *supra* note 67.

⁶⁹ Appendix [XX online]

⁷⁰ Appendix [XX online]

⁷¹ 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->

been embroiled in a range of legal controversies.⁷²

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.⁷³ A number of state regulators are also actively policing bad actors in the ICO market.⁷⁴

has-exploded/ [https://perma.cc/28LB-TYM2] (documenting over 500 exchanges).

⁷² 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).

⁷³ At first, the SEC moved gingerly in response to the novelty of the ICO form, leaving open the question 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., Complaint, SEC v. Plexcorps, 17-CV-7007, 2017 U.S. Dist. LEXIS 206145 (E.D.N.Y., Dec. 14, 2017); Munchee Inc., SEC File No. 3-18304, Release No. 10445 (Dec. 11, 2017), <https://www.sec.gov/litigation/admin/2017/33-10445.pdf>

[https://perma.cc/63QB-6CRB] (order instituting cease-and-desist proceedings); Sec. Exch. Comm’n, Release No. 81207, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (2017), <https://www.sec.gov/litigation/investreport/34-81207.pdf> [https://perma.cc/6PEA-BEMZ]. 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).

⁷⁴ 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->

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.⁷⁵ 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 understand better some of the basic economics of cryptoassets, and the roles that code—specifically, smart contracts—might be playing. The central relationship we investigate is between “paper” and “code.”⁷⁶ 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,” which might render the protections offered by the former to be at best superfluous.⁷⁷

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 888,888ETH hard cap,”⁷⁸ of automated

conduct-coordinated-international-crypto-crackdown-2/
[<https://perma.cc/XC7D-WSPY>].

⁷⁵ See, e.g., Rohr & Wright, *supra* note 18; 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 (2018).

⁷⁶ 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.

⁷⁷ Szabo, *supra* note 6.

⁷⁸ Monaco, White Paper 8 (2017), <https://cryptorating.eu/whitepapers/Monaco/monaco-whitepaper.pdf> [https://perma.cc/YSB2-GF36] (last visited Feb. 4, 2019).

destruction of excess cryptoasset supply,⁷⁹ and of “Reserve Tokens . . . locked in a smart contract” according to predetermined specifications.⁸⁰ They promise with precision that “new founders’ tokens [are] distributed pursuant to the launch of an EOSIO Platform in a smart contract and releases 100,000,000 of such tokens . . . linearly to Block.one every second over a period of 10 years.”⁸¹ While markets of unsophisticated investors typically require investor protection laws and intermediaries to protect against market manipulation,⁸² the “crypto industry” has “greater transparency, fewer middle men . . . [and] programmatically enforceable contracts.”⁸³ 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 not⁸⁴—legal rights are only as valuable as their practical enforceability.⁸⁵ Because cryptoassets can move freely and pseudonymously through the Internet, it can be difficult to pin them down to particular

⁷⁹ Monetha, White Paper 35--36 (June 2017), https://ico.monetha.io/Monetha_WP.pdf [<https://perma.cc/WE6M-859F>].

⁸⁰ Monaco, *supra* note 78, at 11.

⁸¹ Frequently Asked Questions, EOS, <https://eos.io/faq> (on file with the Columbia Law Review) (last visited Feb. 4, 2019).

⁸² See, e.g., I Louis Loss, Joel Seligman, & Troy Paredes, *Fundamentals of Securities Regulation* at 3-4 (6th ed., 2011).

⁸³ Jesse Powell, Kraken’s Position on Regulation, Kraken (Apr. 22, 2018), <https://blog.kraken.com/post/1561/krakens-position-on-regulation/> [<https://perma.cc/K5WY-6PQR>].

⁸⁴ See *supra* text accompanying notes 33--35, 62--75.

⁸⁵ 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.”).

jurisdictions.⁸⁶ 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.⁸⁷ Thus, promises that are made in marketing documents and 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 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, VC vetters, and regulators with teeth—it is the immutable, transparent code that enables (and creates) a trustless but trusted market.⁸⁸ 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

⁸⁶ See, e.g., Receiver's Initial Status Report for Receivership Estate of Arisebank, SEC v. Arisebank, No. 3:18-cv-0186-M (Feb. 26, 2018) (ECF No. 53) (detailing a receiver's difficulties in recovering cryptoassets).

⁸⁷ See *id.*; SEC Office of Investor Education and Advocacy, SEC Pub. No. 153 (7/13), Investor Alert: Ponzi Schemes and Virtual Currency (July 23, 2013), https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf [<https://perma.cc/AKC6-R59V>]; David Z. Morris, The Rise of Cryptocurrency Ponzi Schemes, *The Atlantic* (May 31, 2017), <https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/> [<https://perma.cc/FJU7-NSYW>].

⁸⁸ See kemane, 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> [[perma](#)]; cf. Timothy C. May, The Crypto Anarchist Manifesto, Activism.net, <https://www.activism.net/cypherpunk/crypto-anarchy.html> [[perma](#)] (last visited Feb. XX, 2019).

solution—the token’s coded rules—to manage agency costs.⁸⁹

One type of bargained-for protection is a constraint on the *supply* of the investment asset for sale. In the traditional IPO-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 affect share price, but not firm value. 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. The protections they desire are found in legal documents such as prospectuses. Traditional corporations act through human agents; those humans are only able to issue as many shares as the corporation’s (amendable) Articles of Incorporation allow. Exploitative issuances are deterred by the common law of fiduciary duty.⁹⁰

Supply constraints matter to cryptoasset investors, as well. Remember, tokens are not typically claims on the enterprise’s residual assets.⁹¹ Rather, they typically provide investors the right to use or govern the actual system whose hypothesized construction is funded by their money.⁹² 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.⁹³ 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.

⁸⁹ For an agency-costs model of the choice between VC and ICO forms, see Chod and Lyandres, *supra* note 32, at 14--24.

⁹⁰ See, e.g., *In re Tri-Star Pictures, Inc.*, 634 A.2d 319 (Del. 1993).

⁹¹ See *supra* note 27 and accompanying text.

⁹² See discussion *supra* text accompanying notes 28--29.

⁹³ 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.

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.⁹⁴ Thus, a purchaser's protection against wanton inflation of supply comes directly from the cryptoasset code.⁹⁵ 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.⁹⁶ 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.⁹⁷

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, i.e., *vesting*.⁹⁸ 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.⁹⁹

⁹⁴ See generally De Filippi & Wright, *supra* note 41.

⁹⁵ 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 37, at 215 (emphasis added).

⁹⁶ Bourveau et al., *supra* note 26, at 19 (using white paper promises of soft cap to predict an increase in price).

⁹⁷ See *infra* note 185 and accompanying text.

⁹⁸ 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>].

⁹⁹ See, e.g., Steven N. Kaplan & Per Strömberg, *Financial Contracting Theory Meets the Real World: An Empirical Analysis of Venture Capital Contracts*, 70

In ICOs, classic options are quite rare, but token vesting promises are common.¹⁰⁰ 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.”¹⁰¹ Another wrote, “[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.”¹⁰²

As with promises regarding supply, vesting promises that are coded are enforced automatically.¹⁰³ Those merely present in marketing materials or paper contracts are less likely to be enforceable.¹⁰⁴ Uncoded vesting promises might (or might not) be present in governing documents of the underlying formal

Rev. Econ. Stud. 281, 282, 292 (2003) (“VC financings commonly utilize both founder vesting and non-compete clauses.”)

¹⁰⁰ 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).

¹⁰¹ 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>].

¹⁰² 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>].

¹⁰³ See *supra* note 6 and accompanying text.

¹⁰⁴ 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 NaPoleonX

Stéphane Ifrah, NaPoleonX Newsletter, http://notifications.napoleonx.ai/napoleonx-update-31/01?utm_campaign=ICO%2022nd%20of%20January&utm_content=66619455&utm_medium=social&utm_source=twitter [<https://perma.cc/S4YA-M9YP>] (last visited Feb. 4, 2019).

organizations. They likely would be located in the employment contracts of the various managers and founders, but, such contracts likely 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.¹⁰⁵

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.¹⁰⁶ 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.¹⁰⁷ Because cryptoassets are defined by

¹⁰⁵ 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>].

¹⁰⁶ 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>].

¹⁰⁷ See Sklaroff, *supra* note 48, at 291.

smart contracts, whether those smart contracts are modifiable should profoundly impact price and receive intense investor scrutiny.¹⁰⁸

A fully-disclosed regime that permitted a token to be modifiable should have uncertain effects on value. On the one hand, no social enterprise 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.¹⁰⁹ 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.¹¹⁰ 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 non-carbonated beverages, or could be used to purchase cola only when you inserted additional fiat currency.¹¹¹ The "rights" you bought would be notional.

¹⁰⁸ 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 Computer (June 25, 2018), <https://www.bleepingcomputer.com/news/security/researchers-last-year-s-icos-had-five-security-vulnerabilities-on-average/#.WzObdfcNjVR.email> [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." (quoting Positive.com)).

¹⁰⁹ 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).

¹¹⁰ See Sklaroff, *supra* note 48, at 300 (providing instances of that hubris meeting its just reward).

¹¹¹ 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).

Surprisingly, until July of 2018, the crypto-industry rarely discussed modification.¹¹² 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.¹¹³ They were, to summarize a long and angry 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 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," or EVM.¹¹⁴ This simulation runs by using both data and code (smart contracts) stored on the Ethereum ledger.¹¹⁵ The smart contracts exist on the Ethereum ledger in a complex, hard-to-read machine language known as

¹¹² 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] ("Furthermore, existing smart contracts may have flaws, or they might need updates to their logic. 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.").

¹¹³ See Jackson Palmer, Twitter Thread, Thread Reader (July 9, 2018), <https://threadreaderapp.com/thread/1016455890294091776.html> [https://perma.cc/QSX7-AM7C] ("Ability to completely and centrally pause transfers . . . Such decentralization. Much farce. . . Some of these contracts include an 'upgrade' capability which also allows them to essentially upgrade/replace the token contract.").

¹¹⁴ 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).

¹¹⁵ Id.

bytecode.¹¹⁶ But they are most commonly written in an intuitive programming language called Solidity.¹¹⁷ Solidity hides the internal details of the EVM and the complex machine language that it processes.¹¹⁸ Before being uploaded to the blockchain, a program called a “compiler” is used to translate the Solidity source code into Ethereum bytecode.¹¹⁹ This Article presents examples in Solidity.

Solidity code contains four major types of entities: variables, functions, events, and modifiers.¹²⁰

- *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.¹²¹
- *Functions* describe the rules by which the smart contract operates, storing discrete chunks of code that perform specific tasks.¹²² Functions are executed (or “called”) by sending a specially formatted transaction to the Ethereum network.¹²³ Functions are identified by a name and a set of parameters or “arguments,” that are the inputs to the function.¹²⁴
- *Events* are signals that a smart contract sends to other applications or smart contracts programmed to receive them.¹²⁵ They act as a form of logging.¹²⁶
- *Modifiers* allow a developer to easily restrict the execution

¹¹⁶ 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>].

¹¹⁷ Cf. id. (“Like many other popular programming languages, Solidity is a high level programming language.”).

¹¹⁸ Id.

¹¹⁹ Id.

¹²⁰ Structure of a Contract, <https://solidity.readthedocs.io/en/v0.5.2/structure-of-a-contract.html> [<https://perma.cc/UD2K-3WDZ>] (last visited Jan. 26, 2019).

¹²¹ Id.

¹²² Id.

¹²³ Id.

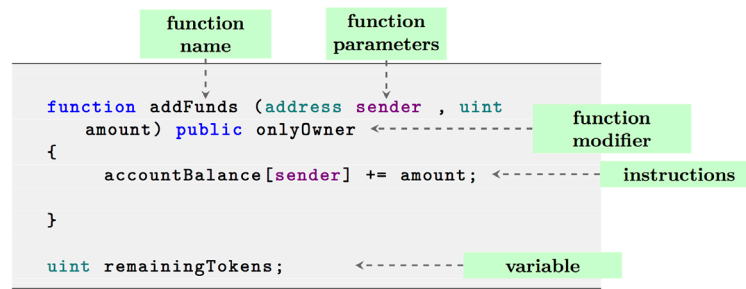
¹²⁴ Id.

¹²⁵ Id.

¹²⁶ See Contracts, <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.”).

of a function under certain conditions.¹²⁷ For example, a developer may restrict the ability to mint new tokens to the smart contract owner alone.¹²⁸

FIGURE 4: An Example Code Snippet¹²⁹



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 display¹³⁰. The site additionally provides a verification feature, which allows users to check that the Solidity code matches the bytecode.¹³¹

¹²⁷ Id.

¹²⁸ See id.

¹²⁹ 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’.

¹³⁰ See What is Etherscan?. Etherscan Support Center, <https://etherscancom.freshdesk.com/support/solutions/articles/35000022140-what-is-etherscan-> [<https://perma.cc/KD78-SSBS>] (last updated Nov. 21, 2017); EtherScan, Contract Verification - Constructor Arguments, Etherscan Support Center, <https://etherscancom.freshdesk.com/support/solutions/articles/35000022165-contract-verification-constructor-arguments> [<https://perma.cc/2FTU-86WD>] (last updated Nov. 21, 2017).

¹³¹ Id. In a few cases, Etherscan did not affirmatively indicate that the uploaded display code as matching the bytecode. In those cases, we did not separately verify the match.

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.¹³² A typical smart contract in our sample consists of 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*.¹³³ Recall that the Ethereum blockchain

¹³² 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 113, 113 (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 241, 241 (Ralf Lämmel ed., 2018). 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.

¹³³ See David Hoffman, Regulating Initial Coin Offerings (ICOs), Penn Wharton Pub. Pol’y Initiative, Oct. 2018, at 2 n.2, <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 37, 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

provides an extremely simple way to mint new cryptoassets through the ERC-20 standard.¹³⁴ But even if they do not conform to the ERC-20 standard, minted assets are typically created by executing relatively simple code on a blockchain.¹³⁵

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.¹³⁶ 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 look at 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.¹³⁷ Like other

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.

¹³⁴ See Hoffman, *Regulating Initial Coin Offerings (ICOs)*, *supra* note 110, at 2; see also *supra* text accompanying notes 54--57. 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 (2017), <https://steemit.com/ethereum/@maxnachamkin/how-to-create-your-own-ethereum-token-in-an-hour-erc20-verified> [<https://perma.cc/A5U5-RDK7>].

¹³⁵ This is not a necessary attribute of minted assets.

¹³⁶ 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.

¹³⁷ Lucas Matney, *Kik Already Has Over 6,000 Bots Reaching 300 Million Registered Users*, TechCrunch (May 11, 2016), <https://web.archive.org/web/20180203034618/https://techcrunch.com/2016/05/11/kik-already-has-over-6000-bots-reaching-300-million-registered-users/> [<https://perma.cc/X62B-NRC8>].

digital communications companies, it has sought to broaden its business model by turning to blockchain.¹³⁸ Ultimately the company would like to build a “decentralized ecosystem of digital services for daily life.”¹³⁹

If all goes according to plan, Kin will be the currency enabling and constituting this utopian ecosystem.¹⁴⁰ 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 membership in “VIP” chat groups with celebrities.¹⁴¹ It will also incentivize developers to work alongside the project.¹⁴²

According to its white paper, Kik planned to mint ten trillion Kin tokens, of which one trillion would be put up for sale.¹⁴³ A blog post from Kik’s founder and CEO states that 488 billion were sold for \$50 million in a pre-sale arranged with specific investors and venture capital funds active in the industry.¹⁴⁴ The remaining 512 billion tokens were offered to the public during the

¹³⁸ 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>] (explaining why rivals are wrong to rely on advertising).

¹³⁹ Id.

¹⁴⁰ 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.”).

¹⁴¹ 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.

¹⁴² 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”).

¹⁴³ Id. at 21.

¹⁴⁴ Ted Livingston, Kin TDE: If You Want to Participate, You *Must* Register by September 9, 9:00 a.m. ET, Kin Blog (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.”).

project's ICO, which ran from September 12--26, 2017.¹⁴⁵ Ultimately, the ICO raised \$98.8 million for the project, bringing the total amount raised to almost \$150 million when including the private presale.¹⁴⁶

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.¹⁴⁷ Figure 5 illustrates the code's function:

FIGURE 5: Kin Project Code¹⁴⁸

¹⁴⁵ 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>; Kik Kik Interactive, Inc., Kin Token Distribution Event Starts Today, Kik <3 Blog (Sept. 12, 2017), <https://www.kik.com/blog/kin-token-distribution-event-starts-today/> [<https://perma.cc/M7Z6-GA7Q>].

¹⁴⁶ See Johnson, Kik Raises \$98 Million, *supra* note 145. 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>].

¹⁴⁷ To purchase tokens, purchaser addresses must be added to a list of participants by Kin's development team. See Ted Livingston, *supra* note 144.

¹⁴⁸ Need cite to Kin projects code.

```

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);
    }
}

```

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.¹⁴⁹ 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.¹⁵⁰ Similarly, a team might alter rules

¹⁴⁹ See supra Figure 5 (setting the max tokens in the first two lines of code).

¹⁵⁰ 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

governing the ICO process to achieve various supply effects. For example, the Kin ICO smart contract contains code to enforce volume restrictions for individual purchasers.¹⁵¹ Each address permitted to participate in the sales may only send a limited amount of ether to the smart contract that disburses KIN tokens.¹⁵² However, these limits could be manually modified by the smart contract owner at any time.¹⁵³

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 cap on the amount of ether that can be created.¹⁵⁴ Indeed there is heated debate about whether this is a desirable feature or not.¹⁵⁵

Supply caps are a typical part of an ICO's marketing materials.¹⁵⁶ 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

Jan. 26, 2019) (explaining Ripple's decision to place 55 billion XRP into a "cryptographically-secured escrow account" to secure XRP).

¹⁵¹ See *supra* Figure 5 (comparing `weiAlreadyParticipated`, the amount of tokens already purchased, with `participationCap`, the total amount allowed to be purchased, and `msg.value`, which contains the requested purchase amount).

¹⁵² See *supra* Figure 5 (creating a cap on ether received).

¹⁵³ 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.

¹⁵⁴ See Ethereum, Ether, <https://www.ethereum.org/ether> [<https://perma.cc/39TF-TDR6>] (last visited Jan. 26, 2019).

¹⁵⁵ 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 @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, reference to the "ice age" difficulty bomb. See Collins, *supra*.

¹⁵⁶ See *infra* Part III & Appendix [XX online]

him any more.”¹⁵⁷

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.¹⁵⁸ When someone pays ether to complete a transaction on the Ethereum blockchain, its recipient can spend that ether right away.¹⁵⁹

But perpetual circulation is not *always* the fate of a cryptoasset. Cryptoassets also can be used up, or “burned”—that is, destroyed.¹⁶⁰ 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.¹⁶¹ In others,

¹⁵⁷ See @dennisk82, Polybius Bank (PLBT Tokens), Steemit (July 12, 2017), <https://steemit.com/crypto/@dennisk82/polybius-bank-plbt-tokens> [<https://perma.cc/T59B-C2NY>].

¹⁵⁸ See Ethereum Whitepaper, *supra* note 47.

¹⁵⁹ See *id.*

¹⁶⁰ 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/#33e9fc8754c4> [<https://perma.cc/V323-SYF2>] (“In its simplest form, burning a token means making the token permanently unspendable.”).

¹⁶¹ See, e.g., FinShi Capital, FinShi Capital Crowdsale Whitepaper 33, 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

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,¹⁶² 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 any tokens or ether sent to that address inaccessible. The below snippet shows a characteristic burning function:

FIGURE 6: Burning Code¹⁶³

```

1      function burn(uint256 _value) public returns (bool success) {
2          require(balanceOf[msg.sender] >= _value);
3          balanceOf[msg.sender] -= _value;
4          totalSupply -= _value;
5          Burn(msg.sender, _value);
6          return true;
7      }

```

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

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.

¹⁶² Every entry (‘block’) on a blockchain is linked to both the entry proceeding 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).

¹⁶³ 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.

Not all burning promises are executed so cleanly. Consider, for instance, Paragon, an ICO that aims to “revolutioniz[e] all things cannabis with blockchain.”¹⁶⁴ Lest you think it’s all a smoky haze (and we promise that’s the last joke), the project does have a dedicated cryptoasset: an ERC-20 token called PRG. The White Paper 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,¹⁶⁵ guide project governance decisions,¹⁶⁶ purchase access to co-working services,¹⁶⁷ and exchange tokens for local currency in cannabis-unfriendly jurisdictions.¹⁶⁸

In addition to these promises about governance, Paragon promised that any unsold tokens from the private or public sale would be burned.¹⁶⁹ And it describes a transaction fee system whereby “all fees on the Paragon ecosystem” incur a \$0.000000005 charge (that’s 5 billionths of a dollar), half of which is burned and half of which replenishes the project’s PRG

¹⁶⁴ 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 co-working spaces for cannabis startups, and engage in widespread pro-legalization advocacy. *Id.* The White Paper 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.

¹⁶⁵ See *id.* at 20.

¹⁶⁶ See *id.* at 21.

¹⁶⁷ See *id.* at 17.

¹⁶⁸ 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 the Matter of 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.com* (Nov. 17, 2018), <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”).

¹⁶⁹ See Paragon Whitepaper, *supra* note 164, at 14.

reserve.¹⁷⁰

We can perceive only a small part of this complex set of rules in the code.¹⁷¹ PRG's smart-contract code does limit issuance to 200 million tokens. This is captured in Figure 7 below:

FIGURE 7: Paragon Supply Code¹⁷²

```
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:

FIGURE 8: Paragon Coin Burning Code¹⁷³

¹⁷⁰ 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.

¹⁷¹ 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 they auditors have inspected the code and “the code does not contain any major flaws... we note the contract charges a fee... which should be made clear.”

¹⁷² Need a cite to Paragon coin code.

¹⁷³ Id.

<pre>// 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; }</pre>	<p>PRG here provides a facility for burning tokens in a manner that registers a decrease in the token supply</p>
--	--

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 in remaining in the supply, causing the eventual demise of the network. This is captured in Figure 9 below:

FIGURE 9: Paragon Fee Code¹⁷⁴

<pre>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; }</pre>	<p>Each PRG transactions is accompanies by a token fee of $supply * 5 * 10^{-11} + 2500$</p> <p>Half of these tokens are permanently removed from the supply, and half are distributed to the owner.</p> <p>Eventually, this leads to a complete depletion of the token supply.</p>
---	--

b. Vesting Promises

If supply controls protect against the threat of dilution, vesting mechanisms protect against the threat of desertion.¹⁷⁵ They work either by delaying when the founder is granted assets,

¹⁷⁴ Id.

¹⁷⁵ See supra note 98 and accompanying text.

or deferring the moment of their liquidity. Vesting typically is provided for using a smart contract that allocates a portion of minted tokens to insiders but then locks them up until some condition is satisfied. The code prohibits the transfer, sale, or use of the tokens until the condition's trip-wire is hit.¹⁷⁶ Most ICO coded vesting is time-based, with few of the contractual conditions that come with stock vesting offline.¹⁷⁷

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."¹⁷⁸ This stake would be subject to a vesting schedule that released ten percent every quarter, for ten quarters.¹⁷⁹

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.¹⁸⁰ This stake vests according to its own schedule.¹⁸¹

¹⁷⁶ 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.

¹⁷⁷ There are, of course, outliers. Aragon, an Ethereum-based platform for building and managing decentralized organizations, claimed that their 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 tokenholders 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 multi-signature smart contract by holders instructed not to execute until the product launches. See Luis Cuende, Aragon, Introducing the Aragon Community Multisig, Aragon 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.

¹⁷⁸ Kik Whitepaper, *supra* note 138, at 21.

¹⁷⁹ *Id.* at 21--22.

¹⁸⁰ *Id.* at 19.

¹⁸¹ See *id.* at 21. These tokens are allocated to fund the Kin Rewards Engine. See *supra* note 142 and accompanying text. Since the amount of tokens being placed in circulation decreases over time, this feature also creates inflation for the token. Kik Whitepaper, *supra* note 138, at 22.

0.061% of this stake will be released into circulation daily, or roughly twenty percent per year.¹⁸² 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 4,601,252,295,287 Kin (that's 4.6 trillion) on March 12, 2019.¹⁸³

FIGURE 10: Kin Allocation Code¹⁸⁴

<pre> 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); } </pre>	<p>This container variable is used to hold values pertaining to a specific grant</p> <p>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.</p>
---	---

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. Grants are both creatable and revocable by the smart-contract owner. No more than 100 grants may ever be created and no address may receive a grant twice. 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.

When the Kin ICO commenced, the developers created two new grants. One corresponds to Kik's 30% stake and faithfully implements the 10% per quarter vesting schedule described in the whitepaper (see Figure 9). Interestingly, the development team manually added a comment to the code showing that the address

¹⁸² Kik Interactive, Inc., Kin Rewards Engine 5 (June 2017), https://kinecosystem.org/static/files/Kin_Rewards_Engine_RFC.pdf [<https://perma.cc/CNG9-TNCF>] [hereinafter Kin Rewards Engine].

¹⁸³ This assuming a January 1, 2018 start date. Kin Rewards Engine 5.

¹⁸⁴ Need cite to Kin Code.

owning the stake belongs to Kik. 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 60% Foundation stake. We were unable to locate code for any of the highly detailed vesting mechanisms described in the white paper. 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 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?

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.¹⁸⁵ 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.¹⁸⁶ Or, think of a public law that points to a private standard, like a city code that adopts LEED green-building standards.¹⁸⁷ The standard can be updated privately, thereby modifying the effect of public law.¹⁸⁸

A similar "pointing" mechanism enables the modification of cryptoasset smart contracts. All tokens using this method shared 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.¹⁸⁹ 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, their current secondary smart-contract address is frozen until the next time they explicitly opt in. The

¹⁸⁵ 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.

¹⁸⁶ 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.").

¹⁸⁷ See Sarah B. Schindler, *Following Industry's LEED: Municipal Adoption of Private Green Building Standards*, 62 *Fla. L. Rev.* 285, 289 (2010).

¹⁸⁸ See *id.* at 303--07 (describing the process by which LEED). 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 188, at 316 (describing the advantages of standards developed in a public system, while recognizing the benefits private regulatory standards provide).

¹⁸⁹ 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.

default state of all users is opt in, as illustrated below.¹⁹⁰

FIGURE 11: Monaco Modification Code¹⁹¹

```
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);
}
```

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.”¹⁹² 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.”¹⁹³ Investors contributing to the project can supposedly expect “higher returns” than those investing in traditional banks.¹⁹⁴

¹⁹⁰ Code for three tokens with modifiable contracts contained copyright notifications in the comments attributing the source to Ambisafe.

```
/**
 * THIS SOFTWARE IS A SUBJECT TO AMBISAFE LICENSE
 * AGREEMENT.
 * NO USE OR DISTRIBUTION IS ALLOWED WITHOUT WRITTEN
 * PERMISSION FROM AMBISAFE.
 * HTTPS://WWW.AMBISAFE.CO/TERMS-OF-USE/
 */
```

¹⁹¹ 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. **Need a cite to Monaco Code.**

¹⁹² Polybius, Polybius Prospectus 1, <https://polybius.io/media/prospectus.pdf> [<https://perma.cc/EG57-QUMY>] (last visited Jan. 26, 2019).

¹⁹³ Id. at 2.

¹⁹⁴ 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

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.¹⁹⁵ 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.¹⁹⁶ 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.

FIGURE 12: Polybius Modification Code¹⁹⁷

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.

¹⁹⁵ Polybius, Polybius Crowdfunding Terms & Conditions 11, https://polybius.io/media/terms_and_conditions.pdf [<https://perma.cc/K7XZ-Y5HM>] (last visited Jan. 26, 2019).

¹⁹⁶ See *id.*

¹⁹⁷ [Cite to Polybius Code.](#)

```

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);
}

```

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 `proposeUpgrade` function.¹⁹⁸ 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 days unless the user opts out.¹⁹⁹ In terms that legal readers will be familiar with, it’s a “sticky default.”²⁰⁰

¹⁹⁸ See *supra* Figure 12.

¹⁹⁹ See *supra* Figure 12.

²⁰⁰ For the classic initial treatment, see generally Omri Ben-Shahar and John E. Pottow, *On the Stickiness of Default Rules*, 33 Fla. St. L. Rev. 651 (2006).

Using these mechanisms, a development team can unilaterally change the tokens purchased by investor—or sometimes, propose changes which will be adopted in a certain percentage of users do not object.²⁰¹ 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 non-technical markers of quality. It's 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).²⁰² For each listed promotion, we scrutinized the white papers, token sale agreements, and computer code posted by the promoters. Appendix [XX] pulls quotes about supply, burning, vesting and modification (if they are available) from the issuers' public statements.²⁰³ We compare those promises, read by investors,

²⁰¹ 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).

²⁰² 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 50 2017 ICOs compiled by Coinschedule, with three notable exceptions. The site omits the Grid+ (<https://gridplus.io/>) ICO, which raised about \$38,500,000 in its pre-sale and ICO, as well as Tron, a controversial project that raised \$70,000,000 in its pre-sale 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 \$42,000,000, does not have an accessible original whitepaper. This made it impossible to determine claims it made about token functionality.

²⁰³ See generally [appendix to be housed online]

with what we discern from close examination of software code. Our approach is empirical, but obviously neither comprehensive nor representative of all 2017 ICOs.

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.²⁰⁴ In the sample, 12 (25%) were headquartered in the United States, 9 (19%) in Switzerland, and the remaining in variety of countries, including Singapore (5), England (2), Russia (2), Estonia (2), and Thailand (2). By January, 2019, 11 of the projects had not released any kind of alpha version or demo of their project.

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."²⁰⁵ 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.²⁰⁶

²⁰⁴ See *infra* Figure 13.

²⁰⁵ What Are Polybius Tokens and Why Should They Be in Every Crypto-Investor's Portfolio?, Steemit <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] (last visited Jan. 27, 2019); see also Polybius Prospectus, *supra* note 192, 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")

²⁰⁶ See Polybius, Polybius Token Whitepaper 4 (May 10, 2017), https://polybius.io/media/token_whitepaper.pdf [https://perma.cc/VV8L-VBXE]; see also Polybius Crowdfunding Terms & Conditions, *supra* note 195, 3 ("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

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' 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 be restricted to relying on vernacular promises.²⁰⁷ This is an excerpt of what the public-facing code (incorporated by reference) looks like:

FIGURE 14: Polybius Bytecode²⁰⁸

```
0x606060405236156100f65763ffffffff60e060020a6000350416
631962df7181146100fb57806319ab453c1461017a5780631a1fea
e1146101a757806321538acb146101c657806324c65f35146101e5
5780633f2f1596146102045780634f6d3aed146102345780635b36
fea61461025357806361d027b3146102725780637a386e88146102
9b5780637afa8388146102c8578063a39385de146102e7578063a4
b7459a14610306578063c10796df14610325578063c358d4ff1461
039b578063cca97025146103cb578063db00b84814610452578063
e34f7137146104bd578063eb58705b146104f4578063ec55688914
610575575b610000565b3461000057604080516020600460443581
```

So it is not merely the case that the investment depends on the development team's decision to actually build product they

calls the dividends "Payouts." Id. at 2. That old-fashioned contract specifies that token holders are "eligible for obtaining [sic] Payouts according to their stakes" and that the token code is "the mechanism of the distribution of Payouts." Id. at 2--3. 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. at 2--4, 11.

²⁰⁷ 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 (Sep. 17, 2017), <https://medium.com/@blockchain101/solidity-bytecode-and-opcode-basics-672e9b1a88c2> [<https://perma.cc/Q4PE-DYBM>].

²⁰⁸ 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. [Cite to Polybius Code.](#)

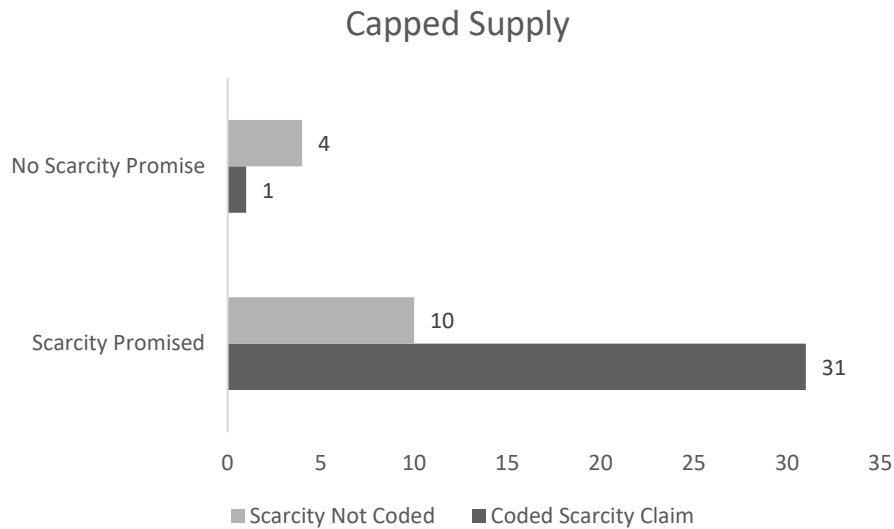
hype in their whitepaper.²⁰⁹ Investors must also have faith—either that ordinary contract law litigation will back up old-fashioned terms of use, or that the bytecode, which essentially no one will or could parse, renders those promises operable.

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 & Burning

We begin with promises regarding supply. Of the fifty tokens, we audited the code of 46 (three remained in bytecode, and one, FileCoin, has not released any code or token). Figure 14 illustrates how such firms approached supply scarcity commitments.

²⁰⁹ 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 EU regulation that was released year 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 Results²¹⁰

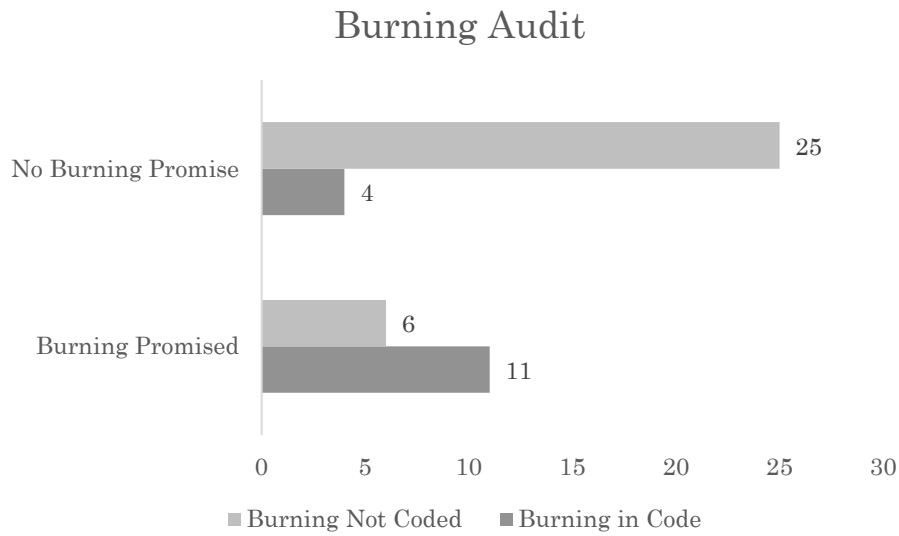
Almost all issuers promise a supply restriction in their marketing documents (41/46 = ~90%). And most of those that promise a restriction deliver it (31/41 = ~75%). Overall, though, only about 2 in 3 (31/46) firms that we audited encoded a supply restriction. To be clear, this is not to say that the 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 Results²¹¹

²¹⁰ Cite to Appendix B.

²¹¹ Cite to Appendix B.



Here, fewer firms promised to burn tokens than promised to cap supply in the initial mint (17 v. 41). Of those that promised to burn supply, 35% (6/17) did not fix that claim with code.

C. Vesting Promises

Of the 46 auditable issuers, only 37 promised vesting in their marketing documents or whitepapers, while 10 did not. Figure 16 illustrates our findings.

FIGURE 16: Vesting Audit Results²¹²

²¹² Cite to Appendix B.

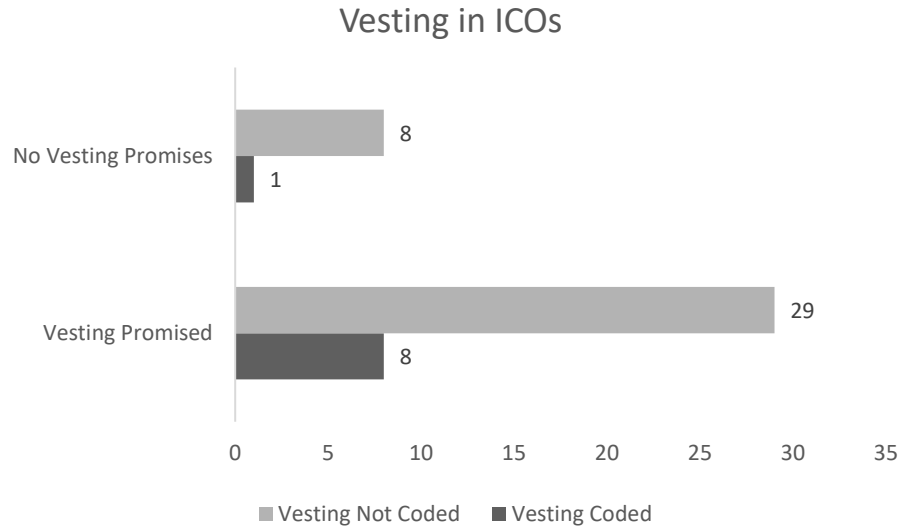
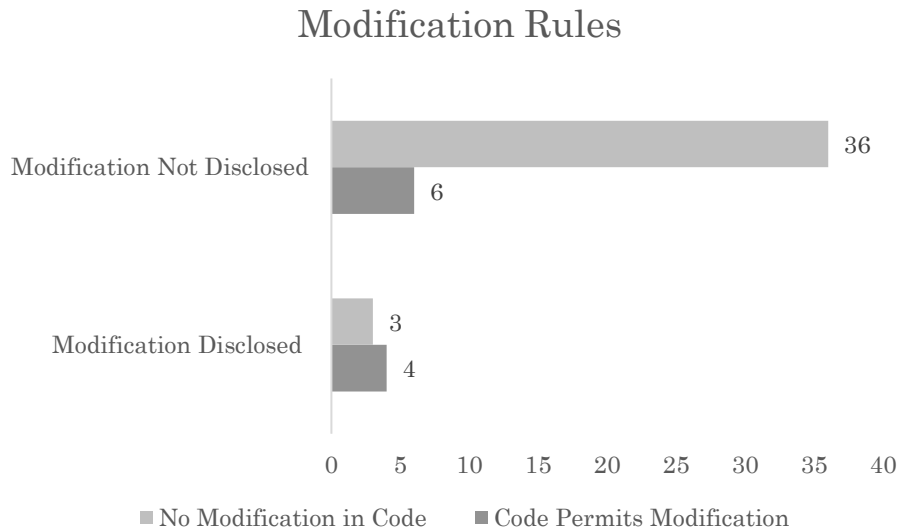


Figure 16 illustrates first that almost 20% of the sample did not promise to vest at all, which is a surprising result given the amounts raised. Second, of the 80% that promised to vest, the vast majority apparently did not use smart contracts to encode those rights.²¹³

D. Modification Promises

Finally, we describe the modification rules in the sample. Modification is rarely discussed in marketing materials: Only 7 of the 50 firms discussed the token’s modifiability in their marketing materials or soft contracts. But overall, 10 of the 50 firms permit modification through their code. While most (4/7) of the firms that disclosed modification had code that backed up their promises, six firms which did not discuss modification permitted it.

²¹³ 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. If we learn that other projects used the BAT structure, we will update this chart accordingly.

FIGURE 17: Modification Audit Results²¹⁴

E. Summary

To sum up: there are significant differences between code and contract in our sample.²¹⁵ 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

²¹⁴ [Cite to Appendix B.](#)

²¹⁵ For the results in summary form, see generally *infra* Appendix B.

traditional law.²¹⁶ We have traced their early history,²¹⁷ explained how they were expected to function in the ICO market of 2017,²¹⁸ and taken stock of the reality.²¹⁹ In this Part, we evaluate the distance between expectations and reality.

As we established in Part III (and 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 restrictions hard-coded into smart contracts. More starkly, we could not find hard-coded vesting restrictions in 29 of the 37 ICOs where promoters promised to adhere to such restrictions. Finally, of ten ICOs where 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

²¹⁶ See De Filippi & Wright, *supra* note 41, 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.").

²¹⁷ See *supra* Part I.

²¹⁸ See *supra* Part II.

²¹⁹ See *supra* Part III.

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.²²⁰ To quantify the idea of paper-code distance, we refer to any uncoded investor protection for supply, burning, or vesting, or incongruence between code and disclosures regarding modifiability as “distance.” Using these data, we score each ICO from zero to four.²²¹ Of the 50 ICOs, we give 49 a score because we can evaluate either the token or the associated smart contracts. Twelve (24%) have no distance, 26 (53 %) have one marker, 9 (18%) have two, 1 (2%) had three, and 1 (2%) has four. If investors know about the problems we’ve identified, then the makeup of the top 50 suggests that they don’t much care.

Nor do the post-sale 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 paper²²² was to develop a rolling weighted portfolio of the prices (and trading volume) of our 50 projects, controlling for their disclosed and coded governance rules. Using this approach, we find that—consistent with earlier work—that disclosed governance rights do seem to promote better returns.²²³

FIGURE 18: Vesting Disclosures & Rolling Average Cumulative Returns²²⁴

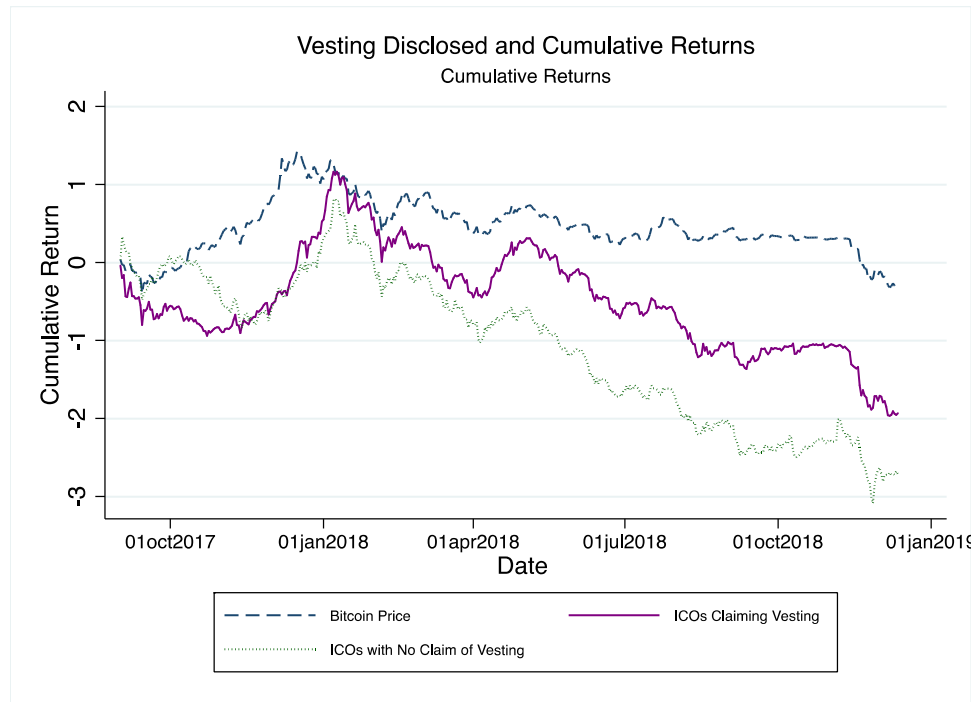
²²⁰ See *infra* Appendix B.

²²¹ 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.

²²² We thank Professor Robert Bartlett for his suggestion and the data which gave it life.

²²³ See *supra* note 31.

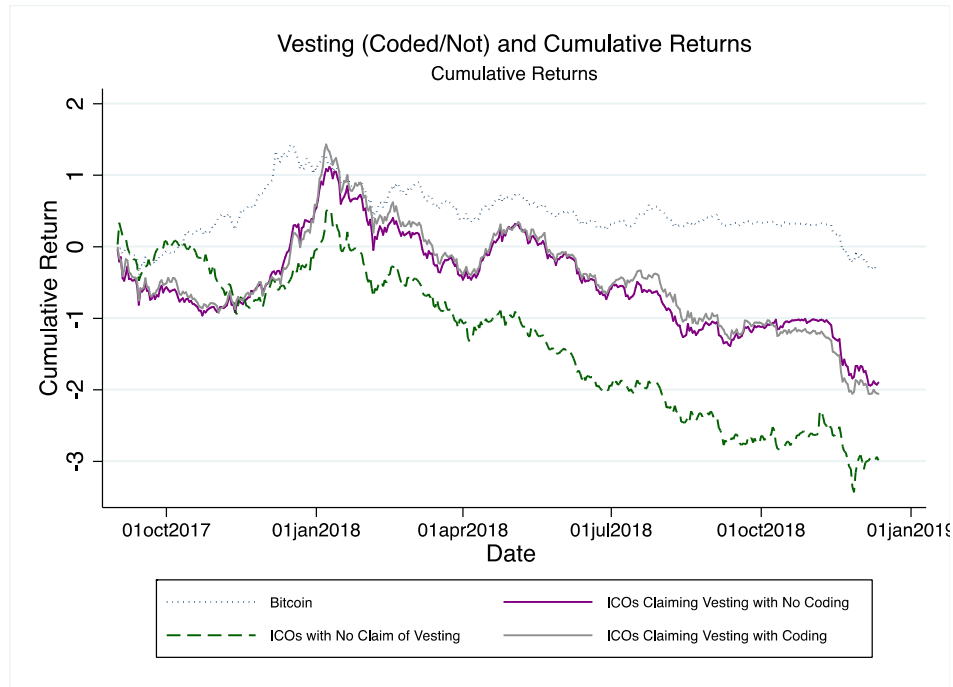
²²⁴ Data from Coinmarketcap, courtesy of Robert Bartlett.



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

FIGURE 19: Vesting (Coded v. Disclosed) & Cumulative Returns²²⁵

²²⁵ Data from Coinmarketcap, courtesy of Robert Bartlett.



Here, we can see that firms that coded vesting had returns which were indistinguishable from those that did not code it. 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 significant effects.²²⁶ Trading volume and price were, rather, closely tied to Bitcoin's price and trading volume, a result that fits with other recent research.²²⁷

Finally, we are skeptical of the "investor-protection code is priced" thesis because buy-side literature in 2016 through 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 top five English-language rating sites by Alexa ranking, only one posts information about code quality, though not of significant detail.²²⁸

²²⁶ On file with the authors.

²²⁷ See Griffith and Shams, *supra* note 8.

²²⁸ 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->

Similarly, code takes a backseat to other investment drivers in the retail valuation literature.

In the period before 2017, advisory publications focused on a projects' ability to deliver anonymity and decentralized governance, which in turn was thought to help hedge against regulation.²²⁹ In the period after, guides focused on the potential for widespread functional use within the startup's system,²³⁰ the reputation and involvement of the founders and creative team,²³¹

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). Only one of the four sites does analyze smart-contract code: icorating.com (Alexa rank: 79,549). 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.

²²⁹ 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/#1af3fc559e22> [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 communally, which run communally or in a decentralized fashion. The more unaffiliated developers contributing to the development and operation of the product, the less likely any profit from the product is to be considered 'from the efforts of others' – and the less likely vertical commonality will be present.").

²³⁰ 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.").

²³¹ 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").

and avoiding obvious scams.²³² Eventually, some investors gave up on ICOs completely.²³³ 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,²³⁴ 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.²³⁵ 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.²³⁶ 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.²³⁷

ICO advocates might reasonably respond this absence of evidence for the importance of code in a number of ways. First, it

²³² 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/#1ac4e7a185ea> [<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.”).

²³³ See *supra* note 19.

²³⁴ Burniske & Tatar, *supra* note 31.

²³⁵ *Id.* at 172--73 (discussing the materials necessary to conduct fundamental analysis of cryptoasset investments).

²³⁶ See, e.g., Reza Jafery, Cryptocurrency Fundamental Analysis: 4 Ways to Gauge the Strength of a Community, *HackeNoon* (Jan. 8, 2018), <https://hackernoon.com/4-ways-to-gauge-the-strength-of-a-cryptocurrencys-community-4b42c0e5d735> [<https://perma.cc/U6QJ-HBQV>]; Simon Kertonegro, 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, Tokenomics and ICO Valuations, *Medium* (Jan. 13, 2018), https://medium.com/@deanpatrick_63570/on-tokenomics-and-ico-valuations-5312e5bdc2bd [<https://perma.cc/V8UH-DNXW>].

²³⁷ Aside from Rhue, *supra* note 36, 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.

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 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.²³⁸ Further, some ICO promoters take to Reddit 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.²³⁹ These audits focus on the antihacking aspects of cybersecurity, not specific instantiation of economically relevant promises.²⁴⁰ But perhaps

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

²³⁹ A Reddit search under https://old.reddit.com/r/ethdev/search?q=ico+audit&restrict_sr=on&sort=relevance&t=all 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>]; Coined, [BUG BOUNTY][ICO] Coined Token Audit (100k EUR Reward!), r/ethdev, Reddit (Oct. 12, 2017), https://old.reddit.com/r/ethdev/comments/75x5kb/bug_bountyico_coined_token_audit_100k_reward/ [<https://perma.cc/4AMQ-TJZP>].

²⁴⁰ See, e.g., Cimpanu, *supra* note 108 (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>]. ICOcheck.io does feature

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.²⁴¹

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 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.²⁴²

crowdsourced evaluations of the presence or absence of smart-contract provisions, including hard-coded vesting constraints. See ICO Checker, icocheck.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.

²⁴¹ 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].

²⁴² These are some of the bodies of paper law that plaintiffs have invoked in their lawsuits against Tezos and Paragon, for instance. See Complaint, Davy v. Paragon Coin, Inc., No. 18-cv-00671 (N.D. Cal., Jan. 1, 2018), 2018 WL 653425; Complaint, Baker v. Dynamic Ledger Solutions, Inc., No. CGC-17-562144 (N.D. Cal. Nov. 20, 2017), 2018 WL 656012; Complaint, Gaviria v.

As we argued above, the legal safeguards against ICO investor exploitation are, at present, significantly weaker than in other investment markets.²⁴³ It is easy for an issuer to set up shop in a low-regulation jurisdiction,²⁴⁴ and the architecture of the cryptoeconomy enables far more user and promoter anonymity than typical markets.²⁴⁵ 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.²⁴⁶ 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*.”²⁴⁷ Smart contract code was, after all, supposed to render traditional intermediaries useless, to obviate the need for regulation, and reduce transactions costs for participants.²⁴⁸ 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

Dynamic Ledger Solutions, Inc., No. 6:17-cv-01959 (M.D. Fla. Nov. 13, 2017), 2017 WL 5713392.

²⁴³ Insert supra cross-reference.

²⁴⁴ See Rohr & Wright, *supra* note 18, at 30--31, 96.

²⁴⁵ See, e.g., John O. McGinnis & Kyle Roche, Bitcoin: Order Without Law in the Digital Age (Northwestern Public Law Research Paper No. 17-06, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=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 (Mar. 10, 2017) (unpublished manuscript), <https://arxiv.org/abs/1703.03779> (on file with the Columbia Law Review); Shifflett & Jones, *supra* note 8.

²⁴⁶ Insert supra cross-reference.

²⁴⁷ Cf. De Filippi & Wright, *supra* note 41, at 193--204 (arguing that ICOs can rely on “*lex cryptographica*” to enforce investor protections).

²⁴⁸ 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).

traditional regulatory tools—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.²⁴⁹

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.²⁵⁰ We simply do not know at the moment enough 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.²⁵¹ 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.²⁵² Others would like the state to keep out.²⁵³ Each approach has costs and benefits, of course—a conundrum where good things

²⁴⁹ 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 (describing briefly the failures in the market that led to the passage of the Securities Act of 1933).

²⁵⁰ See *supra* Part III.

²⁵¹ See, e.g., Messari Disclosures Registry, Messari, <http://messari.io/registry> [on file with the Columbia Law Review] (last visited Jan. 27, 2019).

²⁵² This has been the approach taken, for instance, by regulators in China and South Korea. See Zetzsche et al., *supra* note 16, at 30--32.

²⁵³ See, e.g., Richard Waters, To Coin a Craze: Silicon Valley's Cryptocurrency Boom, Financial 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. 304, 333--40 (2017) (arguing for a light hand on smart contract regulation).

like innovation, investor protection, and regulatory clarity sit uneasily alongside each other.²⁵⁴ 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 grandparents risking their retirement savings?²⁵⁵ Or are they day-traders enjoying a virtual casino?²⁵⁶ We might want—ok, we *do* want—to protect mistaken elders more than thrill-seekers.²⁵⁷ 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.²⁵⁸ 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.

²⁵⁴ See generally Christopher Brummer & Yesha Yadav, Fintech and the Innovation Trilemma, 107 Geo. L.J. (2019 forthcoming), <https://ssrn.com/abstract=3054770> (on file with the Columbia Law Review) (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).

²⁵⁵ 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> [<https://perma.cc/V5H5-CV8N>].

²⁵⁶ 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/3EB2-6Y EJ>] (last updated Sept. 1, 2018).

²⁵⁷ 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).

²⁵⁸ See, e.g., Sean Foley, Jonathan R. Karlson & Talis J. Putnins, Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?, Rev. Fin. Stud. (forthcoming) (manuscript at 1), <https://ssrn.com/abstract=3102645> (on file with the Columbia Law Review).

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.”²⁵⁹ 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.²⁶⁰

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.²⁶¹ ICObench, however, has been accused of operating as a “pay to play” operation.²⁶² Indeed, many rating platforms at the heart of the

²⁵⁹ Popper, *supra* note 10 (quoting Chris Burniske, an industry analyst). For industry post-mortems, on the alleged financial bubble see *supra* notes 14 and 19.

²⁶⁰ See *supra* note 31 (describing the existing literature that explores the influence of various factors on market performance).

²⁶¹ See Momtaz, *supra* note 31, at 31 (defining management team quality); *id.* at 21 (management team quality is 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).

²⁶² See Filip Poutintsev, Beware of ICO Bench!, Medium (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>].

ICO informational ecosystem²⁶³ operate on a “pay to be rated” model.²⁶⁴ 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.²⁶⁵ Such paid systems have well-known

²⁶³ 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>]; WHA Project, We Are Rated by ICO Bench Experts Now!, Steemit (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 Mar. 30, 2018) (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 ICObench FAQ *supra*. 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 Cryptorated, ICO Rating System, <https://cryptorated.com/ico-ratings-calculator/> [[permahttps://perma.cc/LR9J-8PZG](https://perma.cc/LR9J-8PZG)], (last visited Jan. 27, 2019). Others have other features. ICO Drops has a “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. ICO Drops, About Us, <http://www.icodrops.com> <https://icodrops.com/about/> [[permahttps://perma.cc/69LZ-WYAD](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> [[permahttps://perma.cc/BKH2-SJ4Z](https://perma.cc/BKH2-SJ4Z)] (last visited Jan. 27, 2019); ICORating, Project Evaluation, <https://icorating.com/methodology/> [<https://perma.cc/SF7G-3CPY>] (last visited Jan. 27, 2019).

²⁶⁴ See Sedgwick, *supra* note 263.

²⁶⁵ 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-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.*

pathologies, as reflected in the credit-ratings experience during the financial crisis. As a result, when academic papers find that some proxy for social “hype” or “buzz” correlate with higher returns,²⁶⁶ we are not heartened. Instead, they only make us worry about targeted ads²⁶⁷ and “pump and dump” cartels that coordinate massive social-media pushes to temporarily inflate

We had little success independently investigating how much a number of popular rating sites charge. Some, ICO Champs, ICO Drops, and Smith + Crown, disclaim any fee-for-rating service. See ICO Champs, Frequently Asked Questions About ICO Champs, <https://www.icochamps.com/#faq-section> [<https://perma.cc/M83W-KKZ2>] (last visited Jan. 27, 2019); ICO Drops, Submit ICO, <https://icodrops.com/submit-ico/> [<https://perma.cc/29VF-6EGP>] (last visited Jan. 27, 2019); Smith + Crown, Privacy Policy, <https://www.smithandcrown.com/faq/> [<https://perma.cc/EU8F-4FQU>] (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 CoinGecko, How Can I Make My ICO Sponsored?, https://support.coingecko.com/knowledge_base/topics/how-can-i-make-my-ico-sponsored [<https://perma.cc/CG9S-5DLS>] (last visited Jan. 27, 2019); ICObench, Premium, <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 ICO Holder, Publish ICO <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 CoinSchedule, The Ultimate ICO Guide, <https://www.coinschedule.com/brochure.html> (on file with the Columbia Law Review) (last visited Jan. 27, 2019); ICO Alert, Consulting, <https://info.icoalert.com/consulting> [<https://perma.cc/L8FL-RWTG>] (last visited Jan. 27, 2019); ICO Rating, ICORating Terms and Conditions, <https://icorating.com/terms-and-conditions/> [<https://perma.cc/PDT9-38RM>] (last visited Feb. 5, 2019); ICO Watch List, Add a New ICO, <https://icowatchlist.com/add-ico> [<https://perma.cc/4U6G-XRYX>] (last visited Jan. 27, 2019).

²⁶⁶ See Bourveau et al., *supra* note 26 at 5; Rhue, *supra* note 31, at 21--23.

²⁶⁷ See Louise Matsakis, The Cryptocurrency Industry Might Actually Benefit from an Ad Ban, *WIRED* (April 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* (March 26, 2018), <https://www.cnn.com/2018/03/26/twitter-bans-cryptocurrency-advertising-joining-other-tech-giants-in-crackdown.html> [<https://perma.cc/39SZ-MU8T>].

prices before selling their tokens to their marks.²⁶⁸

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.²⁶⁹ 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.”²⁷⁰ 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 80% in 2018,²⁷¹ and trading of certain coins has essentially stopped

²⁶⁸ See Griffin and 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, Business 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, *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).

²⁶⁹ Lee et al., *supra* note 31, at 23, 30--31 (acknowledging that the “insanity of crowds” might be at work).

²⁷⁰ 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.”).

²⁷¹ 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).

completely.²⁷² Research that identifies the particular sources of air for the bubble will be valuable going forward.²⁷³

²⁷² See Deceased Coins, Dead Coins, <https://deadcoins.com/> [<https://perma.cc/Z4KF-99BE>] (last visited January 27, 2019) (listing 680 cryptocurrencies as “deceased,” along with another 182 as “scams”); see also Jay Adkisson, 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).

²⁷³ It seems worth noting that we have observed a number of instances where 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), <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 pre-sale often will dwarf the amount sold in its ICO. Thus, for instance, though Paragon announced its launch with a \$50 million capital raise including pre-sale placements, the SEC recently entered into a consent judgment finding only around \$12 million in total was raised. See *supra* note 168.

Second, there is 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, *Medium* (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)

In a sense, a bubble would be the least surprising, and most manageable explanation of the ICO market's rapid price swings. Regulators would simply need to focus on popping future bubbles with better informational requirements. But the "animal spirits" of irrational exuberance are not the only plausible drivers of ICO demand.²⁷⁴

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.²⁷⁵ Some of these illicit holders might be 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.²⁷⁶ Others might not have politics

(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.

²⁷⁴ 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).

²⁷⁵ See 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."); 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.")₂.

²⁷⁶ Satoshi Nakamoto, *Re: Bitcoin P2P E-Cash Paper*, Cryptography Mailing List (Nov. 7, 2008), <https://www.mail->

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.²⁷⁷ Recently, it has been made salient by allegations that Russian hacking of the Democratic National Committee in 2016 was bought and paid for using Bitcoin.²⁷⁸ Indeed, one recent paper found that approximately *half* of all bitcoin transactions were associated with some form of illegal activity.²⁷⁹ Another found that the imposition of “Know Your Customer” policies designed to enforce tax and anti-money laundering laws shrank ICO returns.²⁸⁰

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 regulatory quietism. 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 helps explain 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

archive.com/cryptography@metzdowd.com/msg09971.html
[https://perma.cc/R8TL-PXRU].

²⁷⁷ 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 percent of all Bitcoin transactions were associated with the Silk Road, an online black market for trade in illegal drugs).

²⁷⁸ 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].

²⁷⁹ Sean Foley, Jonathan R. Karlsen & Tālis J. Putniņš, *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?* 2 (Dec. 15, 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645 (on file with the Columbia Law Review).

²⁸⁰ 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.”).

treating all ICOs like new printings of black-market money. If this is the case, then the high-flying business plans found in ICO white papers 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 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,”²⁸¹ 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.²⁸² That is, it is easier to imagine investing in

²⁸¹ 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>].

²⁸² 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).

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.^{182F²⁸³} 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 warchests from the proceeds of their token sales were eventually forced to liquidate them as the price of Ethereum dropped. This intensified price declines in not only Ethereum but tokens as well.²⁸⁴ If research continues to bear out this effect, it 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.²⁸⁵ Sometimes, they invest directly, as

²⁸³ See Christian Masiak, Joern H. Block, Tobias Masiak, Matthias Neuenkirch, & Katja N. Pielen, *The Market Cycles of ICOs, Bitcoin, and Ether* (pincite), (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3198694 (on file with the Columbia Law Review).

²⁸⁴ See, e.g., Angel Reyes, *Ethereum ICO Funds Liquidation Reaches All-Time High as December Ends* (Dec. 31, 2018), <https://cryptoiq.co/ethereum-ico-funds-liquidation-reaches-all-time-high-as-december-ends/>; Joseph Young, *Did ICOs Cause Ethereum to Drop by 44% in 2 Weeks by Dumping on the Market?* (Aug. 14, 2018), <https://www.ccn.com/did-icos-cause-ethereum-to-drop-by-44-in-2-weeks-by-dumping-on-the-market/>; c.f. Larry Cermak, *ICOs are not Liquidating their ETH Treasuries, Despite Price Declines. Yet.* (Nov 20, 2018), <https://www.theblockcrypto.com/2018/11/20/icos-are-not-liquidating-their-eth-treasuries-despite-price-declines-yet/>

²⁸⁵ See, e.g., Olga Kharif & Camila Russo, *Venture Capital Surges Into Crypto Startups*, Bloomberg (Mar. 26, 2018),

with the participation of Sequoia Capital, Andreessen Horowitz, and Union Square Ventures in the Filecoin ICO.²⁸⁶ 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 crypto asset class.²⁸⁷ 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 raise numerous questions for researchers and regulators, alike. First, recall our 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 towards a fundamental valuation. So, too, does the participation of institutional investors on the long and short sides of the market. These investors do the heavy analytical lifting that helps protect retail investors from succumbing to irrationality. And (most of the time) these investors *read the investment contracts*.²⁸⁸

Are “smart money” investors playing similar channeling roles in the ICO market? It is hard to say. Maybe investors like Sequoia

<https://www.bloomberg.com/news/articles/2018-03-26/icos-can-wait-venture-capital-surges-into-crypto-startups> [https://perma.cc/3UQ5-66AM]; 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].

²⁸⁶ 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].

²⁸⁷ 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].

²⁸⁸ 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> [perma] (patiently 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.”).

Capital are entering into side letters with ICO teams to contractually ensure that supply and vesting promises are upheld.²⁸⁹ Maybe the Andreessen Horwitzes of the world are scrutinizing modifiability, and hold 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.²⁹⁰ 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 riding its coattails. And yet, this doesn’t mean that smart contracts are meaningless.

As John Maynard Keynes (didn’t) say, “the market can stay

²⁸⁹ The Storj secondary vesting contract, discussed *infra* at note 513, would provide a different (and more transparent) way to accomplish the same end.

²⁹⁰ 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/info into prices as it is in securities and commodities markets.

irrational longer than you can stay solvent.”²⁹¹ But over a long enough time horizon, 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 last century. That boom featured massive reallocations of investment capital towards nearly any company that proposed a business strategy that incorporated what was then called the “world wide web.”²⁹² The same has been observed in relation to “blockchain”- and “token”-based business plans in today’s climate.²⁹³ 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.²⁹⁴ Short-term performance on these metrics turned out to have little relation to a company’s long-term success.²⁹⁵

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 to its hopeful participants 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

²⁹¹ See Jason Zweig, Keynes: He Didn’t Say Half of What He Said. Or Did He?, *Wall St. J.* (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].

²⁹² See Elizabeth Demers & Baruch Lev, A Rude Awakening: The Internet Shakeout in 2000, 6 *Rev. Accounting Stud.* 331, 335 (2001).

²⁹³ See, e.g., Nicole Bullock & Robin Wigglesworth, Blockchain Fervour Evokes Memories of Dotcom Bubble, *Fin. Times* (Dec. 18, 2017) [perma] <https://www.ft.com/content/40ec964a-e429-11e7-8b99-0191e45377ec>.

²⁹⁴ See *id.*

²⁹⁵ See *id.*

have gone belly-up, but e-commerce represents 40% of sales for even classic footprint companies like J.Crew,²⁹⁶ and leading apparel start-ups like Everlane and Rent the Runway are decidedly “online-native.”²⁹⁷ And though the grocery deliverer Webvan.com was widely derided as one of the biggest flops of the dot-com bust,²⁹⁸ Amazon is pushing in that direction. The rush for eyeballs has become a rush for data, and online shopping continues its remarkably paced growth.²⁹⁹

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. These animal spirits cause huge amounts of mischief. It ought to be—and indeed is—the province of lawmakers and regulators to temper them.³⁰⁰ 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

²⁹⁶ See J. Crew, Revenues & Sales, eMarketer Retail (2018), <https://retail-index.emarketer.com/company/data/5374f24d4d4afd2bb444660d/5374f2814d4afd824cc159d6/lfy/false/jcrew-revenues-sales> [<https://perma.cc/REP5-PENE>].

²⁹⁷ 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).

²⁹⁸ 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).

²⁹⁹ See Ali Hortaçsu & Chad Syverson, The Ongoing Evolution of US Retail: A Format Tug-of-War, 29 J. Econ. Perspectives 89, 96 (2015) (putting e-commerce in context and documenting its nominal eleven-fold increase between 2000 and 2014).

³⁰⁰ One implication of our paper is that regulatory agencies might investigate the costs and benefits of requiring that cryptocurrencies match their marketing materials to their smart contracts.

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.

Conclusion: The Smart Contract as Artifact

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.³⁰¹ 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—in which 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.

³⁰¹ See Suchman, *supra* note 24, at 92.

Befitting their relatively informal production setting, smart contracts have been ripe for quality control problems. They suffer vast amounts of hacking,³⁰² and, as we show, standards as to how code is produced and made legible are wanting.³⁰³ Unlike the traditional legal world, there are no guilds or expert institutions governing smart contract coders' practices at present 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 suggests that the rate of innovation within smart contracting is driven by social factors, as well as technological ones.³⁰⁴ 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 even *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,"³⁰⁵ is increasingly

³⁰² See Irrera, *supra* note 240 ("More than 10 percent of funds raised through 'initial coin offerings are lost or stolen in hacker attacks.'").

³⁰³ See *supra* Part III.

³⁰⁴ Cf. Kevin Davis, *Contract as Technology*, 88 NYU L. Rev. 83, 86-88 (2013) (encouraging scholars to study innovation in contracting outside traditional domains).

³⁰⁵ 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].

active in patrolling the scene. Other regulators, along with courts, will also contribute to increasing formalization of ICO code standards. The rise of trusted intermediaries appears to be the next necessary step in the maturation of this revolutionary financial form.

Appendix A: Summary of ICOs Audited

FIGURE 13: 50 2017 ICOs³⁰⁶

ICO Name	Country	Announced Raise (\$M) ³⁰⁷	ICO Date ³⁰⁸	Initial Market Value (\$M) ³⁰⁹	Market Value 12/31/2018 (\$M) ³¹⁰
Filecoin		\$257.0 ³¹¹	9/10/17 ³¹²	N/A ³¹³	N/A ³¹⁴
Tezos		\$232.0 ³¹⁵	7/13/17 ³¹⁶	\$1,138.6 ³¹⁷	\$281.0 ³¹⁸
EOS Stage 1		\$185.0 ³¹⁹	6/11/17 ³²⁰	\$654.9 ³²¹	\$2,326.3 ³²²

³⁰⁶ 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.

³⁰⁷ This column represents the total amount of capital that public sources state was raised through each ICO.

³⁰⁸ This column represents the last day of the ICO period for each ICO.

³⁰⁹ This column represents the first reported market capitalization for each ICO. The date is different for each ICO and is indicated parenthetically.

³¹⁰ This column represents the reported market capitalization for each ICO as of December 31, 2018.

³¹¹ Filecoin, ICOMarks, <http://icomarks.com/ico/filecoin> [<http://perma.cc/4QH2-8U6M>] (last visited Jan. 24, 2019).

³¹² Id.

³¹³ Filecoin, CoinMarketCap, <http://coinmarketcap.com/currencies/filecoin/historical-data/> [<http://perma.cc/39NT-7VYN>] (last visited Jan. 24, 2019) (no market capitalization has yet been announced).

³¹⁴ Id.

³¹⁵ Tezos, ICOMarks, <http://www.icomarks.com/ico/tezos> [<http://perma.cc/5SF2-2PTG>] (last visited Jan. 24, 2019).

³¹⁶ Id.

³¹⁷ 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).

³¹⁸ Id.

³¹⁹ EOS, ICOMarks, <http://icomarks.com/ico/eos> [<http://perma.cc/VW96-QA8H>] (last visited Jan. 24, 2019).

³²⁰ Id.

³²¹ 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, 2018).

³²² Id.

Paragon		\$50.0 ³²³	10/15/17 ³²⁴	\$18.7 ³²⁵	\$10.9 ³²⁶
Bancor		\$153.0 ³²⁷	6/12/17 ³²⁸	\$98.8 ³²⁹	\$38.6 ³³⁰
Kin Kik		\$98.0 ³³¹	9/26/17 ³³²	\$88.0 ³³³	\$28.7 ³³⁴
Status		\$100.0 ³³⁵	6/20/17 ³³⁶	\$194.9 ³³⁷	\$59.8 ³³⁸
Tron		\$70.0 ³³⁹	9/2/17 ³⁴⁰	\$29.2 ³⁴¹	\$1,254.5 ³⁴²
TenX		\$80.0 ³⁴³	6/24/17 ³⁴⁴	\$115.4 ³⁴⁵	\$28.3 ³⁴⁶

³²³ Paragon Coin, ICOmarks, <http://icomarks.com/ico/paragon-coin> [<http://perma.cc/Z3N6-XMUX>] (last visited Jan. 24, 2019).

³²⁴ Id.

³²⁵ 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 November 5, 2017).

³²⁶ Id.

³²⁷ Bancor, ICOmarks, <http://icomarks.com/ico/bancor> [<http://perma.cc/V3WG-H2PG>] (last visited Jan. 24, 2019).

³²⁸ Id.

³²⁹ 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).

³³⁰ Id.

³³¹ Kin, ICOmarks, <http://icomarks.com/ico/kin> [<http://perma.cc/EWX2-XU5G>] (last visited Jan. 24, 2019).

³³² Id.

³³³ 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 September 27, 2017).

³³⁴ Id.

³³⁵ Status, ICOmarks, <http://icomarks.com/ico/status> [<http://perma.cc/Y4HV-3PU7>] (last visited Jan. 24, 2019).

³³⁶ Id.

³³⁷ 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).

³³⁸ Id.

³³⁹ Tron, CoinGecko, <http://www.coingecko.com/en/ico/tron> [<http://perma.cc/R5RQ-HSNF>] (last visited Jan. 24, 2019).

³⁴⁰ Id.

³⁴¹ 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 September 28, 2017).

³⁴² Id.

³⁴³ TenX, ICOmarks, <http://icomarks.com/ico/tenx> [<http://perma.cc/U8ZQ-CD8B>] (last visited Jan. 24, 2019).

³⁴⁴ Id.

³⁴⁵ 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).

³⁴⁶ Id.

MobileGo		\$53.0 ³⁴⁷	5/25/17 ³⁴⁸	\$139.2 ³⁴⁹	\$51.3 ³⁵⁰
KyberNetwork		\$49.0 ³⁵¹	9/15/17 ³⁵²	\$254.8 ³⁵³	\$20.6 ³⁵⁴
MCAP		\$44.3 ³⁵⁵	5/7/17 ³⁵⁶	\$29.9 ³⁵⁷	\$0.1 ³⁵⁸
Loopring		\$45.0 ³⁵⁹	8/16/17 ³⁶⁰	\$42.4 ³⁶¹	\$31.5 ³⁶²
Enigma		\$45.0 ³⁶³	9/11/17 ³⁶⁴	\$51.9 ³⁶⁵	\$21.6 ³⁶⁶

³⁴⁷ MobileGo, ICOmarks, <http://icomarks.com/ico/mobilego> [<http://perma.cc/DH2Z-L58N>] (last visited Jan. 24, 2019).

³⁴⁸ Id.

³⁴⁹ 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).

³⁵⁰ Id.

³⁵¹ KyberNetwork, ICOmarks, <http://icomarks.com/ico/kybernetwork> [<http://perma.cc/AKN3-CJQA>] (last visited Jan. 24, 2019).

³⁵² Id.

³⁵³ 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 September 24, 2017).

³⁵⁴ Id.

³⁵⁵ MCAP, ICOmarks, <http://icomarks.com/ico/mcap> [<http://perma.cc/693A-REQS>] (last visited Jan. 24, 2019).

³⁵⁶ Id.

³⁵⁷ 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).

³⁵⁸ Id.

³⁵⁹ Loopring, ICOmarks, <http://icomarks.com/ico/loopring> [<http://perma.cc/H9CM-FJMU>] (last visited Jan. 24, 2019).

³⁶⁰ Id.

³⁶¹ 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 September 2, 2017).

³⁶² Id.

³⁶³ Enigma, ICOmarks, <https://www.icomarks.com/ico/enigma-catalyst> [<https://perma.cc/R2TX-CGSR>] (last visited Feb. 2, 2019).

³⁶⁴ Id.

³⁶⁵ 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 October 14, 2017).

³⁶⁶ Id.

ICON		\$45.0 ³⁶⁷	9/22/17 ³⁶⁸	\$1,976.4 ³⁶⁹	\$112.0 ³⁷⁰
PeerBanks		\$42.6 ³⁷¹	9/22/17 ³⁷²	N/A ³⁷³	N/A ³⁷⁴
Electroneum		\$40.0 ³⁷⁵	10/20/17 ³⁷⁶	\$349.8 ³⁷⁷	\$64.0 ³⁷⁸
Aeternity		\$24.4 ³⁷⁹	6/19/17 ³⁸⁰	\$100.6 ³⁸¹	\$90.6 ³⁸²
Monetha		\$37.0 ³⁸³	8/31/17 ³⁸⁴	\$61.1 ³⁸⁵	\$4.2 ³⁸⁶

³⁶⁷ ICON, ICOMarks, <https://www.icomarks.com/ico/icon> [<https://perma.cc/3CM9-7T7X>] (last visited Feb. 2, 2019).

³⁶⁸ Id.

³⁶⁹ 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 December 25, 2017).

³⁷⁰ Id.

³⁷¹ PeerBanks, ICOMarks, <https://www.icomarks.com/ico/peerbanks> [<https://perma.cc/GJ5N-GLVX>] (last visited Feb. 2, 2019).

³⁷² Id.

³⁷³ No market capitalization data for PeerBanks was available from publicly available coin-focused websites because PeerBanks has not yet been listed on an exchange. See PeerBanks IRA, Tweet (Feb. 8, 2018, 8:16 PM) <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.”).

³⁷⁴ See supra note 373.

³⁷⁵ Electroneum, ICOMarks, <https://www.icomarks.com/ico/electroneum> [<https://perma.cc/G472-FXK5>] (last visited Feb. 2, 2019).

³⁷⁶ Id.

³⁷⁷ 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 December 14, 2017).

³⁷⁸ Id.

³⁷⁹ Aeternity, ICOMarks, <https://icomarks.com/ico/aeternity> [<https://perma.cc/SXQ6-CJAE>] (last visited January 24, 2019).

³⁸⁰ Id.

³⁸¹ Aeternity, CoinMarketCap, <https://coinmarketcap.com/currencies/aeternity/historical-data/?start=20130428&end=20190124> [<https://perma.cc/K5AD-ZDLJ>] (last visited January 24, 2019) (reported as of September 8, 2017).

³⁸² Id.

³⁸³ Monetha, ICOMarks, <https://www.icomarks.com/ico/monetha> [<https://perma.cc/GG2J-G67Y>] (last visited Feb. 2, 2019).

³⁸⁴ Id.

³⁸⁵ Monetha, CoinMarketCap, <https://coinmarketcap.com/currencies/monetha/historical-data/?start=20130428&end=20190124> [<https://perma.cc/PQ8E-QS9V>] (last visited January 24, 2019) (reported as of September 6, 2017).

³⁸⁶ Id.

Basic Attention		\$15.0 ³⁸⁷	5/31/17 ³⁸⁸	\$171.0 ³⁸⁹	\$156.9 ³⁹⁰
Stox		\$33.0 ³⁹¹	8/4/17 ³⁹²	\$36.0 ³⁹³	\$0.6 ³⁹⁴
Civic		\$33.0 ³⁹⁵	6/22/17 ³⁹⁶	\$60.0 ³⁹⁷	\$17.5 ³⁹⁸
Request Network		\$32.9 ³⁹⁹	10/17/17 ⁴⁰⁰	\$36.7 ⁴⁰¹	\$15.4 ⁴⁰²
Grid+		\$32.2 ⁴⁰³	12/12/17 ⁴⁰⁴	\$35.8 ⁴⁰⁵	\$1.8 ⁴⁰⁶

³⁸⁷ Basic Attention Token, ICOMarks, <https://icomarks.com/ico/basic-attention> [<https://perma.cc/982X-8JZG>] (last visited January 24, 2019).

³⁸⁸ Id.

³⁸⁹ Basic Attention Token, CoinMarketCap, <https://coinmarketcap.com/currencies/basic-attention-token/historical-data/?start=20130428&end=20190124> [<https://perma.cc/P3JK-3W92>] (last visited January 24, 2019).

³⁹⁰ Id.

³⁹¹ Stox, ICOMarks, <https://icomarks.com/ico/stox> [<https://perma.cc/2Q42-GJN3>] (last visited January 24, 2019).

³⁹² Id.

³⁹³ Stox, CoinMarketCap, <https://coinmarketcap.com/currencies/stox/historical-data/?start=20130428&end=20190124> [<https://perma.cc/L3BU-AC8T>] (last visited January 24, 2019) (reported as of August 5, 2017).

³⁹⁴ Id.

³⁹⁵ Civic, ICOMarks, <https://icomarks.com/ico/civic> [<https://perma.cc/57KQ-HRFY>] (last visited January 24, 2019).

³⁹⁶ Id.

³⁹⁷ Civic, CoinMarketCap, <https://coinmarketcap.com/currencies/civic/historical-data/?start=20130428&end=20190124> [<https://perma.cc/K2GC-34W8>] (last visited January 24, 2019) (reported as of July 17, 2017).

³⁹⁸ Id.

³⁹⁹ Request Network, ICOMarks, <https://icomarks.com/ico/request-network> [<https://perma.cc/CH84-KXJ5>] (last visited January 24, 2019).

⁴⁰⁰ Id.

⁴⁰¹ Request Network, CoinMarketCap, <https://coinmarketcap.com/currencies/request-network/historical-data/?start=20130428&end=20190124> [<https://perma.cc/Z3KU-M55T>] (last visited January 24, 2019) (reported as of October 20, 2017).

⁴⁰² Id.

⁴⁰³ Grid+, ICODrops, <https://icodrops.com/grid/> [<https://perma.cc/M6GT-LB2U>] (last visited January 24, 2019).

⁴⁰⁴ Id.

⁴⁰⁵ Grid+, CoinMarketCap, <https://coinmarketcap.com/currencies/grid/historical-data/?start=20130428&end=20190124> [<https://perma.cc/6UBQ-XUSG>] (last visited January 24, 2019) (reported as of November 13, 2017).

⁴⁰⁶ Id.

ChainLink		\$32.0 ⁴⁰⁷	9/19/17 ⁴⁰⁸	\$66.2 ⁴⁰⁹	\$101.3 ⁴¹⁰
Polybius		\$31.0 ⁴¹¹	6/30/17 ⁴¹²	\$12.8 ⁴¹³	\$3.9 ⁴¹⁴
Unikoin Gold		\$28.6 ⁴¹⁵	10/23/17 ⁴¹⁶	\$15.8 ⁴¹⁷	\$3.0 ⁴¹⁸
DomRaider		\$45.0 ⁴¹⁹	10/9/17 ⁴²⁰	\$16.8 ⁴²¹	\$1.1 ⁴²²
Blackmoon		\$30.0 ⁴²³	10/12/17 ⁴²⁴	\$25.3 ⁴²⁵	\$3.8 ⁴²⁶

⁴⁰⁷ ChainLink, ICODrops, <https://icodrops.com/chainlink/> [<https://perma.cc/CWZ2-EJZS>] (last visited January 24, 2019).

⁴⁰⁸ Id.

⁴⁰⁹ Chainlink, CoinMarketCap, <https://coinmarketcap.com/currencies/chainlink/historical-data/?start=20130428&end=20190124> [<https://perma.cc/97VG-FDA6>] (last visited January 24, 2019) (reported as of September 20, 2017).

⁴¹⁰ Id.

⁴¹¹ Polybius, ICOMarks, <https://icomarks.com/ico/polybius> [<https://perma.cc/5NV3-U8LQ>] (last visited January 24, 2019).

⁴¹² Id.

⁴¹³ Polybius, CoinMarketCap, <https://coinmarketcap.com/currencies/polybius/historical-data/?start=20130428&end=20190124> [<https://perma.cc/VA5C-XVV6>] (last visited January 24, 2019) (reported as of July 15, 2017).

⁴¹⁴ Id.

⁴¹⁵ Unikoin Gold, ICOMarks, <https://icomarks.com/ico/unikrn> [<https://perma.cc/869H-YA4Z>] (last visited January 24, 2019).

⁴¹⁶ Id.

⁴¹⁷ Unikoin Gold, CoinMarketCap, <https://coinmarketcap.com/currencies/unikoin-gold/historical-data/?start=20130428&end=20190124> [<https://perma.cc/J8M7-4NJX>] (last visited January 24, 2019) (reported as of November 21, 2017).

⁴¹⁸ Id.

⁴¹⁹ DomRaider, ICOMarks, <https://icomarks.com/ico/domraider> [<https://perma.cc/5MH8-QHZK>] (last visited January 24, 2019).

⁴²⁰ Id.

⁴²¹ DomRaider, CoinMarketCap, <https://coinmarketcap.com/currencies/domraider/historical-data/?start=20130428&end=20190124> [<https://perma.cc/R2LV-CACL>] (last visited January 24, 2019) (reported as of November 6, 2017).

⁴²² Id.

⁴²³ Blackmoon, ICOMarks, <https://icomarks.com/ico/blackmoon> [<https://perma.cc/Y6EX-L7DM>] (last visited January 24, 2019)

⁴²⁴ Id.

⁴²⁵ Blackmoon, CoinMarketCap, <https://coinmarketcap.com/currencies/blackmoon/historical-data/?start=20130428&end=20190124> [<https://perma.cc/5L3R-QQPN>] (last visited January 24, 2019) (reported as of September 20, 2017).

⁴²⁶ Id.

Bankera Pre-ICO		\$150.9 ⁴²⁷	2/27/18 ⁴²⁸	N/A ⁴²⁹	N/A ⁴³⁰
Agrello		\$35.0 ⁴³¹	8/17/17 ⁴³²	\$34.5 ⁴³³	\$3.3 ⁴³⁴
Storj		\$30.0 ⁴³⁵	5/25/17 ⁴³⁶	\$23.5 ⁴³⁷	\$19.3 ⁴³⁸
Eidoo		\$28 ⁴³⁹	10/16/17 ⁴⁴⁰	\$25.5 ⁴⁴¹	\$22.3 ⁴⁴²
Monaco		\$26.7 ⁴⁴³	6/18/17 ⁴⁴⁴	\$23.9 ⁴⁴⁵	\$35.3 ⁴⁴⁶

⁴²⁷ Bankera, ICOMarks, <https://icomarks.com/ico/bankera> [<https://perma.cc/4CQU-L6VF>] (last visited January 24, 2019).

⁴²⁸ Id.

⁴²⁹ Bankera, CoinMarketCap, <https://coinmarketcap.com/currencies/bankera/historical-data/?start=20130428&end=20190124> [<https://perma.cc/MT7H-CVHV>] (last visited January 24, 2019) (no market capitalization yet reported).

⁴³⁰ Id.

⁴³¹ Agrello, ICOMarks, <https://icomarks.com/ico/agrello> [<https://perma.cc/M8QM-FEPB>] (last visited January 24, 2019).

⁴³² Id.

⁴³³ Agrello, CoinMarketCap, <https://coinmarketcap.com/currencies/agrello-delta/historical-data/?start=20130428&end=20190124> [<https://perma.cc/DA72-2RW9>] (last visited January 24, 2019) (reported as of September 9, 2017).

⁴³⁴ Id.

⁴³⁵ Storj, ICOMarks, <https://icomarks.com/ico/storj> [<https://perma.cc/WK6J-W4ZR>] (last visited January 24, 2019).

⁴³⁶ Id.

⁴³⁷ Storj, CoinMarketCap, <https://coinmarketcap.com/currencies/storj/historical-data/?start=20130428&end=20190124> [<https://perma.cc/UX89-8YXN>] (last visited January 24, 2019) (reported as of July 2, 2017).

⁴³⁸ Id.

⁴³⁹ Eidoo, ICOMarks, <https://icomarks.com/ico/eidoo> [<https://perma.cc/5JMZ-JBCQ>] (last visited January 24, 2019).

⁴⁴⁰ Id.

⁴⁴¹ Eidoo, CoinMarketCap, <https://coinmarketcap.com/currencies/eidoo/historical-data/?start=20130428&end=20190124> [<https://perma.cc/D68K-KBQU>] (last visited January 24, 2019) (reported as of October 17, 2017).

⁴⁴² Id.

⁴⁴³ Monaco, ICODrop, <https://icodrops.com/monaco/> [<https://perma.cc/JGG8-PRE9>] (last visited January 24, 2019).

⁴⁴⁴ Id.

⁴⁴⁵ Crypto.com, CoinMarketCap, <https://coinmarketcap.com/currencies/crypto-com/historical-data/?start=20130428&end=20190124> [<https://perma.cc/XYD8-66RL>] (last visited January 24, 2019) (reported as of July 3, 2017).

⁴⁴⁶ Id.

Power Ledger		\$13.2 ⁴⁴⁷	10/6/17 ⁴⁴⁸	\$76.6 ⁴⁴⁹	\$32.0 ⁴⁵⁰
Everex		\$26.7 ⁴⁵¹	8/31/17 ⁴⁵²	\$31.5 ⁴⁵³	\$4.4 ⁴⁵⁴
Decentraland		\$24.0 ⁴⁵⁵	8/8/17 ⁴⁵⁶	\$18.7 ⁴⁵⁷	\$47.7 ⁴⁵⁸
FunFair		\$20.0 ⁴⁵⁹	6/23/17 ⁴⁶⁰	\$348.3 ⁴⁶¹	\$22.9 ⁴⁶²
BitClave		\$25.5 ⁴⁶³	11/29/17 ⁴⁶⁴	\$81.7 ⁴⁶⁵	\$0.3 ⁴⁶⁶

⁴⁴⁷ Power Ledger, ICOMarks, <https://icomarks.com/ico/power-ledger> [<https://perma.cc/F4E6-7TA5>] (last visited Jan. 24, 2019).

⁴⁴⁸ Id.

⁴⁴⁹ 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 November 6, 2017).

⁴⁵⁰ Id.

⁴⁵¹ Everex, ICOMarks, <https://icomarks.com/ico/everex> [<https://perma.cc/3BVJ-FW6P>] (last visited Jan. 24, 2019).

⁴⁵² Id.

⁴⁵³ 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 October 10, 2017).

⁴⁵⁴ Id.

⁴⁵⁵ Decentraland, ICOMarks, <https://icomarks.com/ico/decentraland> [<https://perma.cc/8QLC-AVFC>] (last visited Jan. 24, 2019).

⁴⁵⁶ Id.

⁴⁵⁷ 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 September 28, 2017).

⁴⁵⁸ Id.

⁴⁵⁹ FunFair, ICOMarks, <https://icomarks.com/ico/funfair> [<https://perma.cc/9NQ9-C6QL>] (last visited Jan. 24, 2019).

⁴⁶⁰ Id.

⁴⁶¹ 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).

⁴⁶² Id.

⁴⁶³ BitClave, ICOMarks, <https://icomarks.com/ico/bitclave> [<https://perma.cc/7JVU-DC8N>] (last visited Jan. 24, 2019).

⁴⁶⁴ Id.

⁴⁶⁵ 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 January 16, 2018).

⁴⁶⁶ Id.

Tierion		\$25.0 ⁴⁶⁷	7/28/17 ⁴⁶⁸	\$81.6 ⁴⁶⁹	\$5.0 ⁴⁷⁰
OmiseGo		\$25.0 ⁴⁷¹	7/23/17 ⁴⁷²	\$42.6 ⁴⁷³	\$189.5 ⁴⁷⁴
Aragon		\$25.0 ⁴⁷⁵	5/17/17 ⁴⁷⁶	\$36.9 ⁴⁷⁷	\$11.2 ⁴⁷⁸
Ox		\$24.0 ⁴⁷⁹	9/15/17 ⁴⁸⁰	\$134.6 ⁴⁸¹	\$163.9 ⁴⁸²
Enjin Coin		\$23.0 ⁴⁸³	10/31/17 ⁴⁸⁴	\$18.7 ⁴⁸⁵	\$28.6 ⁴⁸⁶
BLOCKv		\$21.5 ⁴⁸⁷	10/25/17 ⁴⁸⁸	\$31.6 ⁴⁸⁹	\$7.2 ⁴⁹⁰

⁴⁶⁷ Tierion, ICOmarks, <https://icomarks.com/ico/tierion> [<https://perma.cc/S44L-P449>] (last visited Jan. 24, 2019).

⁴⁶⁸ Id.

⁴⁶⁹ 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 August 27, 2017).

⁴⁷⁰ Id.

⁴⁷¹ OmiseGo, ICOmarks, <https://icomarks.com/ico/omisego> [<https://perma.cc/N7G3-YV8M>] (last visited Jan. 24, 2019).

⁴⁷² Id.

⁴⁷³ 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).

⁴⁷⁴ Id.

⁴⁷⁵ Aragon, ICOmarks, <https://icomarks.com/ico/aragon> [<https://perma.cc/DB26-QH48>] (last visited Jan. 24, 2019).

⁴⁷⁶ Id.

⁴⁷⁷ 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).

⁴⁷⁸ Id.

⁴⁷⁹ Ox, ICOmarks, <https://icomarks.com/ico/0x> [<https://perma.cc/K6MJ-ZDCN>] (last visited Jan. 24, 2019).

⁴⁸⁰ Id.

⁴⁸¹ Ox, 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 August 16, 2017).

⁴⁸² Id.

⁴⁸³ Enjin Coin, ICOmarks, <https://icomarks.com/ico/enjin-coin> [<https://perma.cc/UY3T-GJB4>] (last visited Jan. 24, 2019).

⁴⁸⁴ Id.

⁴⁸⁵ <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 November 15, 2017).

⁴⁸⁶ Id.

⁴⁸⁷ BLOCKv, ICOmarks, <https://icomarks.com/ico/blockv> [<https://perma.cc/68GU-VQM4>] (last visited Jan. 24, 2019).

⁴⁸⁸ Id.

⁴⁸⁹ 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 December 7, 2017).

⁴⁹⁰ Id.

FinShi Capital		\$21.4 ⁴⁹¹	10/6/17 ⁴⁹²	N/A ⁴⁹³	N/A ⁴⁹⁴
UTRUST		\$20.0 ⁴⁹⁵	11/20/17 ⁴⁹⁶	\$68.1 ⁴⁹⁷	\$10.0 ⁴⁹⁸
Target Coin		\$20.7 ⁴⁹⁹	8/31/17 ⁵⁰⁰	\$28.8 ⁵⁰¹	\$0.8 ⁵⁰²
ATB Coin		\$20.4 ⁵⁰³	9/1/17 ⁵⁰⁴	\$35.2 ⁵⁰⁵	\$0.4 ⁵⁰⁶
Giga Watt		\$15.0 ⁵⁰⁷	7/31/17 ⁵⁰⁸	\$4.3 ⁵⁰⁹	\$1.6 ⁵¹⁰
<i>Total</i>		<i>\$2,584.0</i>	<i>N/A</i>	<i>\$6,967.6</i>	<i>\$5,335.0</i>

⁴⁹¹ FinShi Capital, ICOMarks, <https://icomarks.com/ico/finshi-capital> [<https://perma.cc/FT72-X3FL>] (last visited Jan. 24, 2019).

⁴⁹² Id.

⁴⁹³ No market capitalization data for FinShi Capital was available from publicly available coin-focused websites.

⁴⁹⁴ See supra note 493.

⁴⁹⁵ UTRUST, ICOMarks, <https://icomarks.com/ico/utruster> [<https://perma.cc/5KVG-YVUT>] (last visited Jan. 24, 2019).

⁴⁹⁶ Id.

⁴⁹⁷ UTRUST, CoinMarketCap, <https://coinmarketcap.com/currencies/utruster/historical-data/?start=20130428&end=20190203> [<https://perma.cc/SWZ8-Y629>] (last visited Feb. 2, 2019) (reported as of December 29, 2017).

⁴⁹⁸ Id.

⁴⁹⁹ Target Coin, ICOMarks, <https://icomarks.com/ico/target-coin> [<https://perma.cc/QGL2-C2R2>] (last visited Jan. 24, 2019).

⁵⁰⁰ Id.

⁵⁰¹ 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 October 7, 2017).

⁵⁰² Id.

⁵⁰³ ATB Coin, ICOMarks, <https://icomarks.com/ico/atb-coin> [<https://perma.cc/L7DV-MNDS>] (last visited Jan. 24, 2019).

⁵⁰⁴ Id.

⁵⁰⁵ ATB Coin, CoinMarketCap, <https://coinmarketcap.com/currencies/atbcoin/historical-data/?start=20130428&end=20190203> [] (last visited Feb. 2, 2019) (reported as of October 7, 2017).

⁵⁰⁶ Id.

⁵⁰⁷ Giga Watt, ICOMarks, <https://icomarks.com/ico/giga-watt> [<https://perma.cc/H4CW-CWNF>] (last visited Jan. 24, 2019).

⁵⁰⁸ Id.

⁵⁰⁹ 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 September 2, 2017).

⁵¹⁰ Id.

Appendix B: Summary of Code/Contract Audit

<i>ICON</i> Name	<i>Scarcity</i> (Y/N) <i>Scarcity Coded</i> (Y/N)	<i>Claimed</i> (Y/N) <i>Claimed Coded</i> (Y/N)	<i>Burning</i> (Y/N) <i>Burning Coded</i> (Y/N)	<i>Vesting</i> (Y/N) <i>Vesting Coded</i> (Y/N)	<i>Modification</i> (Y/N) <i>Modification Coded</i> (Y/N)
<i>Filecoin</i>	N/A ⁵¹¹		N/A	N/A	N/A
<i>Tezos</i>	ScarcityNN		BurningNN	VestingYN	ModificationNN
<i>EOS Stage 1</i>	ScarcityNN		BurningNN	VestingYN	ModificationNN
<i>Paragon</i>	ScarcityYY		BurningNY	VestingNN	ModificationNN
<i>Bancor</i>	ScarcityYN		BurningYY	VestingYN	ModificationNN
<i>Kin Kik</i>	ScarcityYY		BurningNN	VestingYY	ModificationNN
<i>Status</i>	ScarcityYN		BurningYY	VestingYY	ModificationYY
<i>Tron</i>	ScarcityYY		BurningNN	VestingYN	ModificationNN
<i>TenX</i>	ScarcityYN		BurningNN	VestingYN	ModificationNN
<i>MobileGO</i>	ScarcityYY		BurningYY	VestingNN	ModificationNN
<i>KyberNetwork</i>	ScarcityYY		BurningYY	VestingYN	ModificationNN
<i>MCAP</i>	ScarcityYY		BurningNN	VestingNN	ModificationNN
<i>Loopring</i>	ScarcityYY		BurningNN	VestingYN	ModificationNN
<i>Enigma</i>	ScarcityYY		BurningYN	VestingYN	ModificationNN
<i>Catalyst</i>					
<i>ICON</i>	ScarcityNY		BurningNY	VestingYN	ModificationNN
<i>PeerBanks</i>	ScarcityYY		BurningNN	VestingNN	ModificationNN
<i>Electroneum</i>	ScarcityYN		BurningNN	VestingYN	ModificationNN
<i>Aeternity</i>	ScarcityYY		BurningYN	VestingYN	ModificationNN
<i>Monetha</i>	ScarcityYY		BurningYY	VestingYY	ModificationNN
<i>Basic</i>	ScarcityYY		BurningNN	VestingYY ⁵¹²	ModificationNN
<i>Attention</i>					
<i>Token</i>					
<i>Stox</i>	ScarcityYY		BurningNY	VestingYY	ModificationNY
<i>Civic</i>	ScarcityYY		BurningNN	VestingYN	ModificationNY
<i>Request</i>	ScarcityYY		BurningYY	VestingNY	ModificationNN
<i>Network</i>					
<i>Grid+</i>	ScarcityYY		BurningYN	VestingYY	ModificationNN
<i>ChainLink</i>	ScarcityYY		BurningNN	VestingNN	ModificationNN

⁵¹¹ 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>].

⁵¹² BAT implements vesting via a secondary smart contract, to which tokens were transferred before the ICO. See <https://etherscan.io/address/0x67fa2c06c9c6d4332f330e14a66bdf1873ef3d2b#code> [<https://perma.cc/A2GE-LWWN>].

<i>Polybius</i>	Unauditable	Unauditable	Unauditable	ModificationYY
<i>Unikoin Gold</i>	ScarcityYY	BurningNN	VestingNN	ModificationNN
<i>DomRaider</i>	ScarcityYY	BurningNN	VestingYY	ModificationNN
<i>Blackmoon</i>	Unauditable	Unauditable	Unauditable	ModificationNY
<i>Crypto Bankera Pre-ICO</i>	ScarcityYN	BurningNN	VestingYN	ModificationNN
<i>Agrello</i>	ScarcityYY	BurningNN	VestingYN	ModificationNN
<i>Storj</i>	ScarcityYY	BurningYY	VestingYN ⁵¹³	ModificationNY
<i>Eidoo</i>	ScarcityYN	BurningYY	VestingYY	ModificationNN
<i>Monaco</i>	ScarcityYN	BurningYN	VestingYN	ModificationNY
<i>Power Ledger</i>	ScarcityYY	BurningNN	VestingYN	ModificationNN
<i>Everex</i>	ScarcityYY	BurningNN	VestingYN	ModificationNN
<i>Decentraland</i>	ScarcityNN	BurningYY	VestingYN	ModificationNN
<i>FunFair</i>	ScarcityYN	BurningYY	VestingYN	ModificationYY
<i>Bitclave</i>	ScarcityYY	BurningYN	VestingYN	ModificationNY
<i>Tierion</i>	ScarcityYY	BurningNN	VestingYN	ModificationNN
<i>OmiseGo</i>	ScarcityYN	BurningYN	VestingYN	ModificationYN
<i>Aragon</i>	ScarcityNN	BurningNY	VestingYY	ModificationYY
<i>0x</i>	ScarcityYY	BurningNN	VestingYN	ModificationNN
<i>Enjin</i>	ScarcityYY	BurningNN	VestingYY	ModificationNN
<i>BlockV</i>	ScarcityYY	BurningNN	VestingYY	ModificationNY
<i>FinShi Capital</i>	Unauditable	Unauditable	Unauditable	ModificationNY
<i>UTRUST</i>	ScarcityYY	BurningYY	VestingYN	ModificationYN
<i>Target Coin</i>	ScarcityYN	BurningNN	VestingNN	ModificationNN
<i>ATB Coin</i>	Unauditable	Unauditable	Unauditable	Unauditable
<i>Giga Watt</i>	ScarcityYN	BurningNN	VestingYN	ModificationYN

⁵¹³ Storj is a hard case. It built a token-based vesting regime outside of its ICO smart contract. See <https://etherscan.io/address/0x34f34f58c50ef059b766065dbb24f7cf885e16463>. 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, see discussion supra note 512) was it completed manually in advance of the ICO.