Coin-Operated Capitalism

Shaanan Cohney
University of Pennsylvania

David A. Hoffman
University of Pennsylvania Law School

Jeremy Sklaroff
University of Pennsylvania

David A. Wishnick
University of Pennsylvania - Center for Technology, Innovation and Competition

Follow this and additional works at: https://scholarship.law.upenn.edu/faculty_scholarship

Part of the Business Law, Public Responsibility, and Ethics Commons, Contracts Commons, Corporate Finance Commons, Entrepreneurial and Small Business Operations Commons, Internet Law Commons, Law and Economics Commons, Political Economy Commons, Science and Technology Law Commons, and the Technology and Innovation Commons

Repository Citation
Cohney, Shaanan; Hoffman, David A.; Sklaroff, Jeremy; and Wishnick, David A., "Coin-Operated Capitalism" (2018). Faculty Scholarship at Penn Law. 2027.
https://scholarship.law.upenn.edu/faculty_scholarship/2027

This Article is brought to you for free and open access by Penn Law: Legal Scholarship Repository. It has been accepted for inclusion in Faculty Scholarship at Penn Law by an authorized administrator of Penn Law: Legal Scholarship Repository. For more information, please contact PennlawIR@law.upenn.edu.
This Article presents the legal literature's first detailed analysis of the inner workings of Initial Coin Offerings. 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 contract-like documents 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 contractual promises. Our inquiry reveals that many ICOs failed even to promise that they would protect investors against insider self-dealing. Fewer still manifested such contracts 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.

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

† 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 in the Center for Technology, Innovation and Competition. We thank Andrew Baker, Tom Baker, Bill Bratton, Chris Brummer, Tony Casey, Peter Conti-Brown, Jill Fisch, Gabe Kaptchuk, Joshua Mitts, Mark Nevitt, Ori Oren, Max Raskin, Usha Rodrigues, Alec Webley, Kevin Werbach, Aaron Wright, participants at the Third Annual Empirical Contracts Conference, and a faculty workshop at Penn for comments. We are immensely grateful for our research assistant partners on this project: Joe Ebb, Kathryn Gardner, Amanda Gould, Taylor Hertzler, Jeffrey Luther, Rachel Mann, Matt Minsky, Hafidzi Razali, and Adam Zuckerman. Address correspondence, including requests for corrections of errors in this draft, to dhoffman@law.upenn.edu.
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. 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. The rise of the Initial Coin Offering (“ICO”) is a chapter in this story, and our subject.1

Obviously, the ICO was named after the IPO, or “Initial Public Offering.” But though the IPO has been familiar for almost a century, the ICO is exotic. Unlike its namesake, an ICO does not typically involve the sale of equity in (or governance rights pertaining to) a corporation.2 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.3 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 related to the supply of the tokens and demand for vended Coke.

1 An introduction to the law, economics, and sociology of peer-to-peer, networked culture begins with YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2007). 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 (2015); Kathryn Judge, The Future of Direct Finance: The Diverging Paths of Peer-to-Peer Lending and Kickstarter, 50 WAKE FOREST L. REV. 603 (2015); Elizabeth Pollman, Information Issues on Wall Street 2.0, 161 U. PA. L. REV. 179 (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.

2 Here, as elsewhere, we make general claims in the text but acknowledge exceptions down below. For instance, ICOs can involve the sale of equity, but it is rare. See discussion infra note 132.

3 While an ICO can occur after a network has been built, the core practice is to raise funds pre-development. See discussion infra Sections II.A-II.B.
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.4

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. 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 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.5

But fraud went hand-in-hand with early financial markets;6 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.7

---

4 Smart contracts were first introduced by Nick Szabo, who drew inspiration from the “humble vending machine,” in Formalizing and Securing Relationships on Public Networks, FIRST MONDAY, Sept. 1997.
In 2017—the year when they entered popular consciousness—
an estimated 200 ICOs raised around $3.8 billion. By July of
2018, an additional 430 ICOs had raised almost $10 billion.

Fourteen billion raised over eighteen months is not chump-
change, but it $2 billion less than what Facebook raised in one
day with its 2012 IPO. 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. To students of capital markets, the interest should be
obvious. One basic question about our new financial contracting

See Nathaniel Popper, Digital Gold: Bitcoin and the Inside
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),
created-icos-and-this-is-the-new-token-hes-backing/#5c0836f01183
(identifying 2017 as the year ICOs became a “runaway trend”).

We address the difficulties of calculating accurate network values
at footnote 189, infra. Solely to ease exposition, in this paper we will generally
use market values (in US dollars) reported by widely used coin data sites.

All data from Coinschedule.com.

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-
of/?mtrref=www.google.com&gwh=6FD71384D902F4F7C941F06F6FAD982D
&gwt=pay.

We join a nascent literature on this topic. See, e.g., Usha Rodrigues, Law
and the Blockchain, 103 IOWA L. REV. (forthcoming 2018); Kevin Werbach,
Trust but Verify: Why Blockchain Needs Law, 32 BERKELEY J.L. & TECH.
(forthcoming 2018); Iris M. Barsan, Legal Challenges of Initial Coin
Offerings, 3 REVUE TRIMESTRIELLE DU DROIT FINANCIER 54 (2017); Dirk A.
Zetzsche, 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.
disclosure failures in a global and rapidly growing market).
world is simple: how are investors protected from exploitation?\footnote{Cf. Darian M. Ibrahim, \textit{Equity Crowdfunding: A Market for Lemons?}, 100 MINN. L. REV. 561 (2015) (describing, and dismissing, worries that crowdfunding markets might be dominated by low-quality startups with few ways to investors to distinguish better ones from the pack).}


Less obviously, an understanding of the ongoing ICO experience can also inform debates about the digital future of capitalism.\footnote{See, e.g., Julie E. Cohen, \textit{The Regulatory State in the Information Age}, 17 THEORETICAL INQUIRIES L. 1 (2016).} 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 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 supply\footnote{Status, The Status Network: A Strategy Towards Mass Adoption of Ethereum at 28 (June 15, 2017), \url{https://status.im/whitepaper.pdf}.} of placing founders’ cryptoasset allocations in “time-locked smart contracts” to align incentives for productivity\footnote{Storj Labs (BVI) LTD., Terms of Token Sale at 14 (May 18, 2017), \url{https://storj.io/sale-terms.pdf}.}; and of “trusted parties replaced with
verifiable computation.” 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.” 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.

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

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 suggest 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. 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.  

22 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 (Hofstra Legal Stud. Res. Paper Series, Res.}
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. In contrast, the ICO method can leave economic ownership and legal control unencumbered.

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, crypto-token pricing should (roughly) reflect an equilibrium between token demand (driven by the present value of expected future exchange options within the token’s native ecosystem) and token supply (driven by the token’s monetary policy).

---


24 See Balaji S. Srinivasan, Thoughts on Tokens, EARN.COM (May 27, 2017), available at https://news.earn.com/thoughts-on-tokens-436109aabcbe. 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 don’t typically divide the formal rights of ownership into pieces.


26 Work on cryptoasset valuation is in its early stages. See, e.g., Catalini & Gans, supra note 21; Aswath Damodaran, The Bitcoin Boom: Asset, Currency,
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 investment bank has backed an ICO. 27 Indeed, the absence of

**Commodity, or Collectible?,** MUSINGS ON MARKETS (Oct. 24, 2017),

27 While venture capitalists have taken cryptoassets into their portfolios, see discussion infra Part 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 Jiri Chod & Evgeny Lyandres, A Theory of ICOs: Diversification, Agency, and Information Failure (unpublished manuscript)
ICO-specific regulation and intermediaries is seen to be a feature, not a bug, by many enthusiasts.28

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.29 ICO transactions augment, and perhaps replace, those mediators by embedding controls within the smart contracts through which rules function.30 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.31 Yet despite their differences, the scenarios share something at a particular level of abstraction: the value of debt, equity, and Colacoin tokens all depend heavily on the success of the entrepreneurial team in building and attracting customers to the product.

B. Understanding Cryptoassets

A working conception of ICOs begins with the cryptoassets—the digital coins and tokens—at the center of the operation. Like a physical coin, a cryptoasset is scarce, and control over it is


29 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)).

30 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).

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). 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.

Cryptoasset history begins with bitcoin currency and the bitcoin ledger (also known as a “blockchain”). Prior to their advent, money was either held in physical form (coins, paper notes), or on the ledger of a centralized intermediary (bank deposits, PayPal balances). Bitcoin is the first significant digital currency system that needs no centralized intermediary to maintain proper books. The key to the ledger’s design—and that of the public blockchain-based systems in its wake—is how it maintains a trustworthy record of ownership rights. Rather than being centralized within a single firm, the bitcoin ledger is replicated and distributed across a network of computers that communicate with each other via the Internet.

---


33 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.


37 See ARVIND NARAYANAN, JOSEPH BONNEAU, EDWARD FELTEN, ANDREW
computers are called “nodes.” 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. Rather, they rely on incentives and code-based controls that govern the nodes’ behavior to ensure that all copies of the ledger are updated identically.

The shift towards a broad range of blockchain-based business plans was realized in another currency network: Ethereum. The designers of Ethereum produced a general-purpose computational system that operates through a public blockchain. 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. 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 that interact with the ledger known as smart contracts. Just as legal contracts govern the allocation of paper money among transactors, smart-contract code governs the transmission of ether, or other assets,

---

38 Narayanan et al., supra note 37, at 7-10.
39 See Werbach, supra note 12, at 24.
40 See Werbach, supra note 12. 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 7. 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.
41 See Werbach & Cornell, supra note 19, at 333-35; Rohr & Wright, supra note 14, at 19.
43 See generally Werbach & Cornell, supra note 19; Jeremy Sklaroff, Comment, Smart Contracts and the Cost of Inflexibility, 166 U. PENN. L. REV. 263 (2017); 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).
among transactors on the Ethereum system. (In most ways, calling these code snippets “contracts” is quite misleading, but we are stuck with the dominant terminology.)

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.⁴⁴ These inputs might include basic information about where to send ether, and also more complex information, like data from a weather vane.⁴⁵ 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 insurance,⁴⁶ escrow,⁴⁷ or even something akin to corporate formation.⁴⁸

To build increasingly complex mechanisms within Ethereum, its community has begun developing coding standards. One of those—standard “ERC-20”⁴⁹—plays a large role in our story. It

---

⁴⁴ It also served as inspiration for Nick Szabo’s initial coinage of the smart-contract idea. See Szabo, supra note 22.
⁴⁸ 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 12.
establishes a simple set of steps to create (or “mint,” in crypto-lingo) entirely new cryptoassets within the Ethereum system. This is what the description of the standard looks like in code:

```solidity
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);
}
```

*Figure 1 - The ERC-20 Interface*

A Cryptoasset that meets the ERC-20 standard contains a block of code for each of the named functions and events above.

Creating a new cryptoasset typically requires a minimum fifty lines of code and three decisions: 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. The next major sale was Augur, in October 2015. The market grew slowly until 2017, when it hit the gas.


As the ICO market has exploded, so too has regulatory interest in its activities. Such scrutiny is no surprise: ICOs, like many Internet-based phenomena before them, intentionally take 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, but the archetypal version is public—democratized, in the tradition of Kickstarter and other “peer-to-peer” financial platforms. *See discussion supra* notes 1, 13. See *Augur: Welcome to the future of forecasting*, ICOBENCH https://icobench.com/ico/augur (last visited July 17, 2018). Between Ethereum in September 2014 and Augur in October 2015, there were several small ICOs that raised under $2 million. *See, e.g.*, *ICOs and Crowdsales: Over $270 Million Raised and Counting*, SMITH & CROWN (Dec. 1, 2016) https://www.smithandcrown.com/icos-crowdsale-history/.
place at the regulatory perimeter.\textsuperscript{52} They exploit a basic tension between the cross-jurisdictional and pseudonymous aspects of cryptocurrency transactions on the one hand and the objectives of regulators on the other.\textsuperscript{53} 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. 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. As of 2017, no similarly clear regime was in place for ICOs. In lieu of the heavily-lawyered products of IPO documentation, the ICO market coalesced on a less formal document known as a “white paper.”\textsuperscript{54}

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. Authoritative copies are typically available in PDF form on promoters’ websites and provided through listing services like coinschedule.com. This makes white papers a transparent form


\textsuperscript{54} See Barsan, supra note 12, at 54.
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. 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. Absent clearly-communicated and defined offers, it is unlikely that buying a token in reliance on such documents constitutes a traditional contract, though other regimes of consumer protection law (state consumer Unlawful Trade Practices statutes, false advertising, securities laws) might fill the regulatory gap.

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

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 are contemplating whether, and to what extent, they should expend scarce resources regulating ICOs. A number of state regulators are also actively policing bad actors in the ICO market.

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. 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

We now seek 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.” By paper, we mean


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.) By code, we mean the blockchains and associated smart contracts that govern the cryptoassets sold through ICOs.

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.60

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,”61 of automated destruction of excess cryptoasset supply,62 and of “Reserve Tokens . . . locked in a smart contract” according to predetermined specifications.63 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.”64 While markets of unsophisticated investors typically require investor protection laws and intermediaries to protect against market manipulation, the “crypto industry” has “greater transparency, fewer middle men . . . [and] programmatically enforceable contracts.”65 That is: this community tries to make concrete the

60 Szabo, supra note 4.
63 Monaco, supra note 61, at 11.
ideological project of using code to replace the rules of entity governance that law currently creates.

Practical realities also motivate a turn to code in this space. Even if the paper surrounding ICOs created legally binding obligations—which it sometimes will not—legal rights are only as valuable as their practical enforceability. Because cryptoassets can move freely and pseudonymously through the Internet, it can be difficult to pin them down to particular jurisdictions. 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. 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 veters, and regulators with teeth—it is the immutable, transparent code that enables (and creates) a trustless but trusted market. 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

66 See supra text accompanying notes 28-30, 53-59.
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 generally must generally suffice. What’s new here (if anything) is that the cryptoasset community proposes a technological solution—the token’s coded rules—to manage agency costs.\footnote{See Chod and Lyandres, supra note 27, at 14-24, for an agency-costs model of the choice between VC and ICO forms.}

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. 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.

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

Electronic copy available at: https://ssrn.com/abstract=3215345
cola, they also pray that Coca-Cola won’t engage in rampant inflation of the token supply.

ICO’s, 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 of a blockchain. Thus, a purchaser’s protection against wanton inflation of supply comes directly from the cryptoasset code. 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. 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.

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. Option, lock-up, and vesting rules attempt to align manager incentives’ with those of the firm, and are endemic in the early-stage VC financing world.

In ICO’s, classic options are quite rare, but token vesting promises are common. As one project (marketing its vesting

72 See generally DE FILIPPI & WRIGHT, supra note 19.
73 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 32, at 215 (emphasis added).
74 Bourveau et al., supra note 21, at 19 (using white paper promises of soft cap to predict an increase in price).
75 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.
76 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
promises) wrote, it “is a governance practice designed to ensure long-term alignment of interests and is standard for any serious project.”

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.”

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

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. Perhaps one reason that options mechanisms are underrepresented is that appropriate strike prices are hard to determine for tokens.


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. Stéphane Ifrah, NaPoleonX: NaPoleonX Update 31/01, Coin Trends (Feb. 1, 2018), https://cointrends.top/news/view/napoleonx-update-31-01-already-8-million-eur-raised-since-our-launch-last-week.

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. 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 drafted in exhaustive, precise code that seems to sets the parties’ obligations permanently. Because cryptoassets are defined by smart contracts, whether those smart contracts are modifiable should profoundly impact price and receive intense investor scrutiny.

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,

blackmoon-financial-group-a-financial-technology-company-founded-56b5a64d88c3 (last visited June 24, 2018).

81 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, Tweet (Apr. 5, 2017, 3:46 PM) https://twitter.com/NTmoney/status/849755116156600321.


83 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 (“Once an ICO starts, the contract cannot be changed and is open to everyone, meaning anyone can view it and look for flaws.”).
evolve. Imagine a constitution that could never be amended, or a similar corporate charter.84 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.85 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.86 The “rights” you bought would be notional.

Surprisingly, until July of 2018, the crypto-industry rarely discussed modification.87 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

---

84 Cf. Henry Hansmann, Corporation and Contract, 8 AM. L. & ECON. REV. 1 (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).

85 Sklaroff, supra note 43, at 300 (providing instances of that hubris meeting its just reward).

86 There are resonances 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, THE MODERN CORPORATION AND PRIVATE PROPERTY 186 (1932) (attacking blank check stock for permitting board entrenchment)).

87 Earlier discussions flew below the radar. Cf. Alan Lu, Programmer, Gnosis, Solidity DelegateProxy Contracts, GNOSIS (May 17, 2018), https://blog.gnosis.pm/solidity-delegateproxy-contacts-e09957d0f201 (“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.”)
modifiable at will. 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 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. This simulation runs by using both data and code (smart contracts) stored on the Ethereum ledger. The smart contracts exist on the Ethereum ledger in a complex, hard-to-read machine language known as byte code. But they are most commonly written in an intuitive programming language called Solidity. Solidity hides the internal details of the EVM and the complex machine language that it processes. Before being uploaded to the blockchain, a program called a “compiler” is used to translate the Solidity source code into Ethereum byte code. We will show you examples in Solidity.

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

- **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.
- **Functions** describe the rules by which the smart contract operates, storing discrete chunks of code that perform specific tasks. Functions are executed (or “called”) by sending a specially formatted transaction to the Ethereum network. Functions are identified by a name

See Jackson Palmer, Twitter Thread (July 9, 2018), https://threadreaderapp.com/thread/1016455890294091776.html (“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.”).
and a set of parameters or “arguments,” that are the inputs to the function.

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

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 byte code present on the blockchain, but requires developers to upload Solidity source code for display. The site additionally provides a verification feature, which allows users to verify that the Solidity code matches the byte code.\(^8^9\)

After obtaining source code, we then examine each function of a smart contract and manually track the role each line plays.

---

\(^{89}\) In a few cases, Etherscan did not list the uploaded display code as matching the byte code. In those cases, we did not separately verify the match.
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. 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. Recall that the Ethereum blockchain provides an extremely simple way to mint new cryptoassets through the ERC-20 standard. But even if they do not conform to the ERC-20 standard, minted assets are typically created by

---

90 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. 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. Two pieces of code written in different programming languages can have the same semantics, while differing in syntax. Semantics is therefore the level at which we attempt to audit the code.

91 An alternative process, known as mining, is often used to create cryptoassets, but not for ICOs. In mining, suppliers of computational power receive cryptoassets in exchange for performing network-critical functions for the blockchains housing the cryptoassets. Bitcoin provides an archetypal example of mining. Bitcoin miners devote processing power to the blockchain, using their computers to solve complex math problems that help verify transactions. The first miner to discover a valid solution can lay claim to the newly mined bitcoin. For further details, see Böhme et al., supra note 32, at 215-218.

92 See supra text accompanying notes 48-50. 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.
executing relatively simple code, on a blockchain.\(^93\)

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.\(^94\) 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.\(^95\) Like other digital communications companies, it has sought to broaden its business model by turning to blockchain.\(^96\) Ultimately the company would like to build a “decentralized ecosystem of digital services for daily life.”\(^97\)

If all goes according to plan, Kin will be the currency enabling and constituting this utopian ecosystem. Building on Kik’s previous efforts to develop in-app loyalty points, Kin is

---

\(^93\) This is not a necessary attribute of minted assets.

\(^94\) 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.

\(^95\) 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//.


\(^97\) Id.
meant to serve as a “transaction currency” that Kik users can exchange for premium features, like membership in “VIP” chat groups with celebrities. It will also incentivize developers to work alongside the project.

According to its white paper, Kik planned to mint ten trillion Kin tokens, of which one trillion would be put up for sale. 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. The remaining 512 billion tokens were offered to the public during the project’s ICO, which ran from September 12-26, 2017. Ultimately the ICO raised $98.8 million for the project, bringing the total amount raised to almost $150 million when including the private presale.

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

---

98 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. See id.
99 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”).
100 Id. at 21.
103 See id. 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, Vice Pres. Of Commc’ns, Kik Interactive, Inc., Maintaining the Kin Token Structure: Redistributing Unsold Kin, r/KinFoundation (2017), https://www.reddit.com/r/KinFoundation/comments/724x9/maintaining_the_kin_token_structure/.
other is presumably the private presale. Figure 5 illustrates the code’s function.

```solidity
def create(address _recipient) public payable onlyDuringSale {
    require(_recipient != address(0));
    uint256 alreadyParticipated = participationHistory[msg.sender];
    uint256 participationCap = SafeMath.min256(participationCaps[msg.sender], hardParticipationCap);
    uint256 cappedWeiReceived = SafeMath.min256(msg.value, participationCap.sub(alreadyParticipated));
    require(cappedWeiReceived > 0);

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

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

    // The 'create' function is run each time ether is transferred to the contract during the ICO – set at 14 days from creation.
    // The final function checks that neither the individual nor the total caps and have been reached and then mints and issues to the sender the appropriate amount of KIN – stored within the contract’s ledger.
```  

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

2. Increasing Supply

The full supply of a minted cryptoasset can be set at the outset of a project, or can fluctuate depending on how much investment the project receives. The *circulating* supply of the

---

104 To purchase tokens, purchaser addresses must be added to a list of participants by Kin’s development team.
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. Similarly, a team might alter rules 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. Each address permitted to participate in the sales may only send a limited amount of ether to the smart contract that disburses KIN tokens. However, these limits could be manually modified by the smart contract owner at any time.105

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. Indeed there is heated debate about whether this is a desirable feature or not.106

Supply caps are a typical part of an ICO’s marketing materials.107 As one promoter said, “Even if on the last day of distribution Richard Branson shows up on a resplendent white yacht packed stern to bow with cash, we wouldn’t be able to sell him any more.”108

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

---

105 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.

106 Despite many attempts to impose a hard cap, there has been no progress. Buterin April Fools Tweet: https://twitter.com/VitalikButerin/status/980744740277661696. Note that ether supply is in some ways determined by the economics of mining, reference to the “ice age” difficulty bomb.

107 See infra Part III & Appendix B.

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

But perpetual circulation is not *always* the fate of a cryptoasset. Cryptoassets also can be used up, or “burned.” 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”—or destroyed—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. In others, only those tokens exchanged for certain features in the product—for example, tokens paid as fees—are burned. Finally, burning is used as a mechanism in ICOs, as a way to destroy unsold supply.

Burning on the Ethereum blockchain takes two forms. The first is a simple transfer of tokens (or ether) to the address of Ethereum’s “genesis” block, consisting of all zeros. As this

---

109 “FinShi Capital takes on the obligation of buying back the tokens through the fund’s profits, thus implementing dividend policy. Once the fund announces an exit from a portfolio company, there will be created a queue of investors who applied for selling their tokens back to the fund. The amount of tokens for buy-back will be announced together with the exit date. The fund will buy out the tokens within one month after the exit from a startup. After that the tokens will be destroyed.” FinShi Capital, FinShi Capital Crowdsale Whitepaper at 18, available at http://finshi.capital/whitepaper_finshi_eng.pdf (last visited June 25, 2018). As 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.

110 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 https://en.bitcoinwiki.org/wiki/Genesis_block
address has no owner, the tokens cannot be spent and as such

Figure 6 - Burning Code

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.

```solidity
function burn(uint256 _value) public returns (bool success) {
    require(balanceOf[msg.sender] >= _value);
    balanceOf[msg.sender] -= _value;
    totalSupply -= _value;
    Burn(msg.sender, _value);
    return true;
}
```

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.

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

Not all burning promises are executed so cleanly. Consider, for instance, Paragon, an ICO that aims to “revolutioniz[e] all things cannabis with blockchain.”\(^1\) (“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. The White Paper describes a ParagonSpace, a Paragon Accelerator, an “immutable ledger for all industry related data.” Of course, all of these efforts are powered by cryptoassets and smart contracts.)

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,\(^2\) guide project governance decisions,\(^3\)

---

\(^1\) Whitepaper 1.
\(^2\) Whitepaper 20
\(^3\) Whitepaper 21
purchase access to co-working services, and exchange tokens for local currency in cannabis-unfriendly jurisdictions.

In addition to these promises about governance, Paragon promised that any unsold tokens from the private or public sale would be burned. 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 reserve.

We can perceive only a small part of this complex set of rules in the code. PRG’s smart-contract code does limit issuance to 200 million tokens. We also verified that Paragon contains code allowing users to burn a portion of their tokens.

114 Whitepaper 23
115 Whitepaper 12
116 Whitepaper 14.
117 Whitepaper 30. 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 there is “severe price volatility” or “excessive sell volume,” making it difficult for investors to value tokens ex ante. 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.
118 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.”
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.

```
uint256 constant INITIAL_TOKENS_COUNT = 2000000000000;

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";
}

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;
}
```

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

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

```
Each PRG transaction is accompanied by a token fee of supply * 5 * 10^-11 + 2500
Half of these tokens are permanently removed from the supply, and half are distributed to the owner.
Eventually, this leads to a complete depletion of the token supply.
```

```
Each PRG transaction is accompanied by a token fee of supply * 5 * 10^-11 + 2500
Half of these tokens are permanently removed from the supply, and half are distributed to the owner.
Eventually, this leads to a complete depletion of the token supply.
```

```
Figure 8 - Paragon Fee Code
```

```
Figure 8 - Paragon Fee Code
```

```
Figure 7 - Paragon Supply Code
```

```
Figure 7 - Paragon Supply Code
```

```
Electronic copy available at: https://ssrn.com/abstract=3215345
```

```
Electronic copy available at: https://ssrn.com/abstract=3215345
```

```
Electronic copy available at: https://ssrn.com/abstract=3215345
```

```
Electronic copy available at: https://ssrn.com/abstract=3215345
```

```
Electronic copy available at: https://ssrn.com/abstract=3215345
```

```
Electronic copy available at: https://ssrn.com/abstract=3215345
```

```
Electronic copy available at: https://ssrn.com/abstract=3215345
```
b. Vesting Promises

If supply controls protect against the threat of dilution, vesting mechanisms protect against the threat of desertion. They work either by delaying when the founder is granted assets, or deferring the moment of their liquidity. Vesting typically occurs 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 determines that the tokens cannot be transferred, sold, or used at all until the condition’s trip-wire is hit.119 Most ICO coded vesting is time-based, with few of the contractual conditions that come with stock vesting offline.120

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.”121 This stake would be subject to a vesting schedule that released ten percent every quarter, for ten quarters.122

Further, sixty percent of the initial Kin was allocated to the Kin Foundation, the entity that is meant to gradually take

---

119 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.
120 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 White Paper, § 5 (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 https://blog.aragon.one/introducing-the-aragon-community-multisig-348a69d16374 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.
121 Whitepaper 21
122 Id. at 21-22.
control of the project. This stake vests according to its own schedule.\textsuperscript{123} 0.061\% of this stake will be released into circulation daily, or roughly twenty percent per year.\textsuperscript{124} 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.\textsuperscript{125}

The project implemented some of these promises in the code. The Kin smart contract creates vesting by maintaining a database of \textit{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.

```
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);
}
```

\textit{Figure 9 - Kin Vesting Code}

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

\textsuperscript{123} These tokens are allocated to fund the Kin Rewards Engine, discussed \textit{supra} note 99. See Whitepaper 19. Since the amount of tokens being placed in circulation decreases over time, this feature also creates inflation for the token. White paper 22.

\textsuperscript{124} Kin Rewards Engine 5.

\textsuperscript{125} This assuming a January 1, 2018 start date. Kin Rewards Engine 5.
team manually added a comment to the code showing that the address 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 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.\textsuperscript{126} 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.\textsuperscript{127} Or, think of a public law that points to a private standard, like a city code that adopts LEED green-building standards.\textsuperscript{128} The standard can be updated privately, thereby modifying the effect of public law.\textsuperscript{129} 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.\textsuperscript{130} 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, 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 default state of all users is opt in, as illustrated below.\textsuperscript{131}

\textsuperscript{126} 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.


\textsuperscript{130} 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.

\textsuperscript{131} Code for three tokens with modifiable contracts contained copyright notifications in the comments attributing the source to Ambisafe.
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.” Eventually, Polybius plans to “grow into your daily servicer and companion ecosystem . . . enabling secure and seamless connections between life and the things we love and use every day.” Investors contributing to the project can supposedly expect “higher returns” than those investing in traditional banks.132

132 Prospectus, 1. The first step in this project was the sale of Polybius tokens (PLBT) to raise money for the Polybius Foundation. PLBT gives holders rights more traditionally associated with stock or other forms of ownership. It promises that holders will have the “right to receive a part of distributable profits of Polybius P.I. or Polybius Bank. All tokens in aggregate will have the right to receive 20% of such profits.” Prospectus, 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 without registration or an applicable exemption from registration.

---

```solidity
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);
}
```

*Figure 10 - Monaco Modification Code*
The development team did make some limited claims about smart contract modification. The token purchase agreement explicitly states that “Polybius shall procure [sic] that the Smart Contract is modified and/or amended via an additional smart contract” to activate tokenholder voting.\(^{133}\) 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.\(^{134}\) 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 11 details.

---

\(^{133}\) Polybius T&C, p.5

\(^{134}\) Polybius T&C, p.5
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. 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. In terms that legal readers will be familiar with,
it’s a “sticky default.”

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. 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). For each listed promotion, we scrutinized the white papers, token sale agreements, and computer code posted by the promoters. Appendix B pulls quotes about supply, burning, vesting and modification (if they are available) from the issuers’

135 For the classic initial treatment, see Omri Ben-Shahar and John E. Pottow, On the Stickiness of Default Rules, 33 FLA. ST. L. REV. 651 (2006).
137 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. https://www.coinschedule.com/icos.html. 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.
public statements. We compare those promises, read by investors, 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 raised a total of $2.6 billion in revenue at their ICOs, and the notional initial market cap was $3.8 billion.

Appendix A provides summary statistics for each ICO in our study. The business sectors in the sample varied, with most being located in infrastructure (14), trading (8), payments (7), and other aspects of finance (5). 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 May, 2018, six 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 teams’ promise that “according to the conditions of the ICO, payouts to tokenholders are directly connected to the earnings of the Polybius project.”\(^{138}\) 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.\(^{139}\)

\(^{138}\) [https://steemit.com/cryptocurrency/@satoshi092/what-are-polybius-tokens-and-why-should-they-be-in-every-crypto-investor-s-portfolio](https://steemit.com/cryptocurrency/@satoshi092/what-are-polybius-tokens-and-why-should-they-be-in-every-crypto-investor-s-portfolio). See also Prospectus at 6 (moneys raised will be used “mainly, but not exclusively on acquisition of licenses, building out the systems, hiring the team and marketing.”)

\(^{139}\) See, e.g., Polybius Token Whitepaper, 4; Polybius terms and conditions, p. 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’s coded governance exists in bytecode (which, as you’ll 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.\textsuperscript{140} This is an excerpt of what the public-facing code (incorporated by reference) looks like:

\begin{verbatim}
0x606060405236156100f65763fffffffff60e6000a000350416
631962df7181146100fb57806319ab453c1461017a5780631a1f6a
e1146101a757806321538acb146101c657806324c65f3516101e5
5780633f2f1596146102045870634f6d3aed146102345780635b36
f6a1461025357806361d027b3146102725780637a386e88146102
9b5780637af8388146102c8578063a39385de46102e7578063a4
b7459a14610306578063c1079ddf14610325578063c358d4ff1461
039b578063cfa97025146103cb578063db00b84814610452578063
e34f71371461046b578063eb58705b146104f4578063ec55688914
610575575b610000565b34610000576040805160206000460443581
\end{verbatim}

Figure 12 - Polybius Bytecode

The main contract incorporates by reference code to perform most tasks. The figure shows an excerpt of the ‘byte code’ referenced. While a skilled analyst can reconstruct the function of the code, such analysis is beyond our scope.

So it is not merely the case that the investment depends on the development team’s decision to actually build product they hype in their whitepaper.\textsuperscript{141} Investors must also have faith—

\textsuperscript{140} Analyzing byte code involves tracing the 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 byte code see \url{https://medium.com/@blockchain101/solidity-bytecode-andOpcode-Basics-672e9b1a88c2}

\textsuperscript{141} Note that the Polybius team actually decided to release a different project than the one described in the white paper. \url{https://cryptocomes.com/past-ico-review-why-you-cant-take-polybius-to-the-bank}. They claimed that this was
either that ordinary contract law litigation will back up old-fashioned terms of use, or that the byte code, which essentially no one will or could parse, renders those promises operable.

Putting unauditible 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 & Burning**

We begin with promises regarding supply. Of the fifty tokens, we audited the code of 46 (three remained in byte code, and one, FileCoin, has not released any code or token). Figure 13 illustrates how such firms approached supply commitments.

![Figure 13: Supply audit, comparing scarcity claims in marketing documents to coding.](https://ssrn.com/abstract=3215345)

Almost issuers promise a supply restriction in their marketing documents ($41/46 = \sim 90\%$). And most of those that promise a restriction deliver it ($31/41 = \sim 75\%$). Overall, though, only about 2 in 3 ($31/46$) firms that we audited encoded a supply restriction. To be clear, we are not saying that the firms that did 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 they want with the funds raised.
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 14 details our burning audit.

![Burning Audit](https://ssrn.com/abstract=3215345)

Here, we can see that 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 White Papers, while 10 did not. Figure 15 illustrates our findings.
Figure 15 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.142

D. Modification Promises

---

142 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.
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.

E. Summary

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

\[\text{For the results in summary form, see Appendix C infra.}\]
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—a snapshot of a supposedly revolutionary innovation just after its birth. Second, we have attempted to understand smart contracts at a deep level of contextual detail. They are at the heart of the innovation story told by ICO proponents, some of whom claim that code will increasingly be able to replace traditional law. We have traced their early history (Part I), explained how they were expected to function in the ICO market of 2017 (Part II), and taken stock of the reality (Part III). In this Part, we evaluate the distance between expectations and reality.

As we established in Part III (and detail in Appendix C), 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 doesn’t 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

---

144 See DE FILIPPI & WRIGHT, supra note 19, at 102-103 (“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.”).
also raises serious questions about whether investors are adequately protected from founder desertion.

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

Though the ICO market is young, we are skeptical of this “investor-protection code is priced” thesis. As a first cut, the sheer number of problems in our sample suggests otherwise. Our results show that the majority of the top-grossing ICOs of 2017 had major problems with how code bore out their anti-exploitation disclosures.145 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 market metrics we are able to observe support the “code is priced” thesis. Let’s test market responses in two exploratory ways: by examining the relationship between code and initial capital raises, and the relationship between code and post-ICO market performance. These are traditional units of analysis in corporate law,146 and they increasingly are used in the latest batch of ICO valuation studies.147 Because the code-auditing process we employed is manual, our sample size is necessarily tiny. But our results are not heartening to the code advocates.

Initial raise. If ICO investors were scrutinizing smart-contract code before buying into an ICO, we would expect to see (all else equal) higher capital raises by teams that faithfully coded supply and vesting protections, and also disclosed their modification powers.148 We find no evidence of that effect in our

145 See infra Appendix C.
147 See supra note 26.
148 An alternative hypothesis, which our data limitations do not permit us to test, is that because the ability to read code is scarce, investors discount the value of all tokens on the market. This lemons hypothesis is intriguing,
ample. To quantify the idea of paper-code distance, we call 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. 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.

We then plot each ICO on two charts relating distance first to initial market value of each ICO, and then to the amount raised. (See Figure 17 below.)

Figure 17: Box Plot of the relationship between market measures and distance. The left figure plots the initial market value per Appendix A; the right figure plots the initial raise.

We see no relationship between the code-disclosure distance we observed in Part III and any initial market measure.

**Post-ICO Performance.** A negative correlation between price appreciation and paper-code distance might suggest that ICO investors were (due to a lack of publicity, or some other aspect of the market) unable to vet code swiftly enough to embed its importance into ICO-period demand, but were able to respond to it as time went on. To conduct this analysis, we first calculate July 31, 2018 network values in terms of percentage of initial

though it does not seem to fit with the qualitative evidence we’ve gathered about valuation, nor the current (2018) sky-high prices we observe.

149 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.

150 Regression results, controlling for time, headquarters, functioning product, and industry type, are also insignificant, but are not sufficiently powered to be meaningful.
post-ICO network values. These range from 82,000% at the high end (meaning that, controlling for supply changes, the cryptoasset was trading at 82x initial value) to 9% at the low end (meaning that investors lost their shirts). The average network value for our sample grew by 375%, and the median growth was 100%.

Table 1 details the lack of a easily-observable relationship between network value appreciation and paper-code distance. Nothing in other empirical literature on ICO performance and pricing—further discussed below—raises suspicions to the contrary.

Table 1: Measures of Quality and Market Performance

<table>
<thead>
<tr>
<th>Number of Uncoded Promises</th>
<th>Mean Ratio of Initial to Final Market Value (Average = 3.75)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>19</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Finally, we are skeptical of the “investor-protection code is priced” thesis because buy-side literature today rarely treats 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. Similarly, code takes

---

151 This strategy is superior to computing the change in cryptoasset prices, as it controls for the effect any supply changes. To conduct the analysis, we create a variable that represents the ratio between the firm’s initial market capitalization and its capitalization as of July 31, 2018, if it is available.
152 In an unreported logit regression, we also find that no quality measure that we identified predicted the firm’s likelihood to be worth less in the present that it was at launch, controlling for firm age, a US headquarters, and whether it had a functioning product as of June 2018. Again, the analysis is underpowered.
153 We identify the top five ratings sites by reference to http://iconow.net/all-ico-calendarlisting-sites-with-alexa-rank-and-traffic/. The four that do not
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 be help hedge against regulation.\(^{154}\) In the period after, guides focused on the potential for widespread functional use within the startup’s system,\(^ {155}\) the reputation and involvement of the founders and creative team,\(^ {156}\) and avoiding obvious scams.\(^ {157}\) There’s little to no emphasis on checking that coded governance actually happens.

analyze smart-contract code are  icodrops.com (Alexa rank: 14,206); icobench.com (Alexa rank: 15,078); coinschedule.com (Alexa rank: 18,861); and cryptopotato.com (Alexa rank: 136,699). The one that does is 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. For instance, in its review of the Mercolet ICO, it mentions neither “smart contracts,” nor “code.”


\(^{154}\) “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,” 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.

“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,” Marco Santori, *Appcoin Law: ICOs The Right Way*, CoinDesk, Oct. 15, 2016, https://www.coindesk.com/appcoin-law-part-1-icos-the-right-way/.

\(^{155}\) “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,” Chinedu Adeyemi, *Cryptocurrency: How to Start? Guide to Cryptocurrency Trading for Beginners*, The Oofy (Jun. 2, 2018), https://theoofy.com/13199/cryptocurrency-how-to-start-guide-to-cryptocurrency-trading-for-beginners/.


\(^{157}\) “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,
For instance, while the bestselling *Cryptoassets: The Innovative Investor’s Guide to Bitcoin and Beyond* does exhort investors to scrutinize developer activity,\(^\text{158}\) 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.\(^\text{159}\) 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.\(^\text{160}\) 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.\(^\text{161}\)

ICO advocates might reasonably respond this absence of evidence for the importance of code in a number of ways. First, it might be the case that investor-protection code will manifest itself as a driver of market returns in the future. Perhaps future researchers will develop measures that capture price tremors in response to phenomena like the one we identified in Part III. It is also possible that the market will increasingly be driven by investors who scrutinize code. Some commentators do advise


\(^{159}\) BURNISKE & TATAR, *supra* note 26, at 172-173 (discussing the materials necessary to conduct fundamental analysis of cryptoasset investments).


\(^{161}\) Aside from Rhue, *supra* note 31, at 20, who finds that identification of “bugs” on Etherscan is associated with lower market capitalization, we are aware of no other analysis of the relationship between code and market value.
investors to pay attention to the underlying code of cryptocurrency projects, and their approach may be gaining adherents. 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. These audits focus on the antihacking aspects of cybersecurity, not specific instantiation of economically relevant promises. But perhaps the recent “modifiability crisis” after the Bancor hack will bring our investor-protection concepts to the fore. In other words, the market will reflect investor protections found in code sooner or later.

162 Rohr and Wright, supra note 14, at 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: “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,” How to Choose An ICO to Invest in, Cointelegraph (2018), https://cointelegraph.com/ico-101/how-to-choose-an-ico-to-invest-in#read-the-white-paper; also, “The quality of a developer can be understood by analyzing some of their code. ... Avoid messy developers,” 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/.


164 See, e.g., Cimpanu, supra note 83 (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.

165 ICOcheck.io does feature crowdsourced evaluations of the presence or absence of smart-contract provisions, including hard-coded vesting
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. 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.\(^{166}\)

As we argued above, the legal safeguards against ICO investor exploitation are, at present, significantly weaker than in other investment markets. It is easy for an issuer to set up shop in a low-regulation jurisdiction,\(^ {167}\) and the architecture of the cryptoeconomy enables far more user and promoter anonymity than typical markets.\(^ {168}\) 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. 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 constraints. See icocheck.com. 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.

\(^{166}\) These are some of the bodies of paper law that plaintiffs have invoked in their lawsuits against Tezos and Paragon, for instance. See Compl., Baker v. Dynamic Ledger Solutions, Inc., No. CGC-17-562144, 2018 WL 656012 (Nov. 20, 2017); Compl., Gaviria v. Dynamic Ledger Solutions, Inc., No. 6:17-cv-01959 (M.D. Fla. Nov. 13, 2017); Compl., Davy v. Paragon Coin, Inc., No. 18-cv-00671 (N.D. Ca., Jan. 1, 2018).

\(^{167}\) See Rohr & Wright, *supra* note 14, at 30-31, 96.

Smart contract code was, after all, supposed to render traditional intermediaries useless, to obviate the need for regulation, and reduce transactions costs for participants. Without those justifications, it becomes harder to see what ICO provides, other than regulatory arbitrage.

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

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. 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. After the publication of this article in draft form, for instance, we learned of several sites which were working to develop informally-rich certification systems. 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. Others would like the state to keep out. Each

---

169 Cf. De Filippi & Wright, supra note 19, at 193-204 (arguing that ICOs can rely on “lex cryptographica” to enforce investor protections).
171 This has been the approach taken, for instance, by regulators in China and South Korea. See Zetzsche et al., supra note 12, at 32-34.
approach has costs and benefits, of course—a conundrum where good things like innovation, investor protection, and regulatory clarity sit uneasily alongside each other. 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? Or are they day-traders enjoying a virtual casino? We might want—ok, we do want—to protect mistaken elders more than thrill-seekers. 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.

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

---

172 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 (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 GEOGETOWN L & TECH REV. 304 (2017) (arguing for a light hand on smart contract regulation).


the sell-side picture we have painted in this Article. Gaining a better read on the precise ratios and combinations of each will be a key next step for scholars and policymakers who deal with ICOs.

1. Irrational Exuberance

The conventional wisdom about ICOs—the meme that drives most headlines—is that we are in the midst 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.” A massive financial bubble would certainly help explain why the market doesn’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.

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

---

177 Popper, supra note 7 (quoting Chris Burniske, an industry analyst).
178 See supra note 26.
179 See Momtaz, Initial Coin Offerings, at 31 (defining management team quality), 21 (management team quality is a “first-order predictor” for ICO success); but see Rhue, supra note 26, at 22-24 (finding no clear link between rating scores and prices).
180 See Filip Poutintsev, Beware of ICO Bench!, Medium (May 13, 2017), https://cryptocurrencyhub.io/beware-of-ico-bench-a41e401b69ea. 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.” Tokenicide, ICObench Warmer (Apr. 24, 2017), https://www.tokenicide.com/opinion/icobench-warmer/.
the ICO informational ecosystem operate on a “pay to be rated” model. 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. Such paid systems have

---


well-known 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,\(^\text{184}\) we are not heartened. Instead, they only make us worry about targeted ads\(^\text{185}\) and “pump and dump” cartels that coordinate massive social-media pushes to temporarily inflate prices before selling their tokens to their marks.\(^\text{186}\)

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.\(^\text{187}\) Cooler heads suggest that taking market returns seriously would be seriously misleading, given the market’s immaturity and “speculative frenzy.”\(^\text{188}\) We are inclined to agree—and to suggest that research that identifies the particular sources of air for the

---

\(^\text{184}\) See Rhue, supra note 31, 21-23; Bourveau et al., supra note 21 at 5.


\(^\text{187}\) Lee et al., supra note 26, at 28-29 (acknowledging that the “insanity of crowds” might be at work).

bubble will be valuable going forward.189

In a sense, a bubble would be the least surprising, and most manageable version of the ICO market we are living through. Regulators would simply need to focus on popping the bubble with better informational requirements. But the “animal spirits” of irrational exuberance are not the only plausible drivers of ICO demand.190

2. Illicit Demand

As 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.191 Some of these illicit holders might be

189 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. Though it is possible to verify that a project’s tokens were transferred to certain wallets at some point before its public sale, there’s 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.

Second, there is no way to link a given Ethereum wallet address to a specific person or institution. Ethereum addresses can be created rapidly and for free. 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.


191 See Ryan Clements, Decoding the Demand for Cryptocurrency: What Is Driving the Historic Price Surge?, The FinReg Blog (Sept. 26, 2017),
inspired by the original, anarcho-capitalist vision for Bitcoin: to “win a major new battle in the arms race and gain a new territory of freedom” from centralized governments.192 Others might not have politics on their mind.

This second “conventional wisdom” about the cryptoasset market was initially suggested by accounts of how bitcoin’s growth was fueled by the drug trade.193 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.194 Indeed, one recent paper found that approximately half of all bitcoin transactions were associated with some form of illegal activity.195 Another found that the imposition of “Know Your Customer” policies designed to enforce tax and anti-money laundering laws shrank ICO returns.196

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 ICO ecosystem who are benefiting from their dalliance with criminal underworlds.

Along with the “bubble demand” hypothesis, the “illicit


193 See Popper, supra note 6 (describing the role of the Silk Road in driving early Bitcoin demand); Reza Raessi, The Silk Road, Bitcoins, and the Global Prohibition Regime on the International Trade in Illicit Drugs, 8 Glendon J. Int’l Stud. (2015) (noting that for a time, 4.5%-9% of all Bitcoin transactions were associated with the Silk Road).


196 See Lee et al., supra note 26, 28.
demand” hypothesis also helps explain some of the results we see. For instance, if criminal payments-facilitation is indeed a major driver of demand for ICOs, then it is unsurprising that investors do not seem to care about whether founder vesting promises are delivered via smart-contract code. Instead, they might simply be treating all ICOs like new printings of black-market money. If this is the case, then the high-flying business plans found in ICO 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,”197 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. That is, it’s easier to imagine investing in speculative assets, without caring too much about the details, when the stake you use 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. This suggests that investors are trading between Ether and Bitcoin on the one hand, and ICOs, on the other. 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. Sometimes, they invest directly, as with the participation of Sequoia Capital, Andreessen Horowitz, and Union Square Ventures in the

---


Filecoin ICO. 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. 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.

Are “smart money” investors playing similar channeling roles in the ICO market? It is hard to say. Maybe investors like Sequoia Capital are entering into side letters with ICO teams to contractually ensure that supply and vesting promises are upheld. 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

---

203 The Storj secondary vesting contract, discussed infra at note 353, would provide a different (and more transparent) way to accomplish the same end.
disclosures.\textsuperscript{204} 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.

\textbf{C. Whose Market Might It Become?}

Based on the strong evidence that smart money is \textit{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 irrational longer than you can stay solvent.”\textsuperscript{205} 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

\textsuperscript{204} 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.

investment capital towards nearly any company that proposed a business strategy that incorporated what was then called the “world wide web.” The same has been observed in relation to “blockchain”- and “token”-based business plans in today’s climate. 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.\(^\text{206}\) Short-term performance on these metrics turned out to have little relation to a company’s long-term success.\(^\text{207}\)

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 have gone belly-up, but e-commerce represents 40% of sales for even classic footprint companies like J.Crew,\(^\text{208}\) and leading apparel start-ups like Everlane and Rent the Runway are decidedly “online-native.” And though the grocery deliverer Webvan.com was widely derided as one of the biggest flops of the dot-com bust,\(^\text{209}\) Amazon is pushing in that direction. The rush for eyeballs has become a rush for data, and online shopping continues its remarkably paced growth.\(^\text{210}\)


\(^{207}\) See id.


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. And yet, we are convinced there is something useful to be learned from this first experiment in blockchain governance. Some firms are encoding their promises though it’s not obviously rewarding to do so. Others are working to create intermediaries and certification regimes despite the contrary incentives present in a sharply rising market. Rewarding such good actors should be as important to regulators as punishing fraudsters.

**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 commerce in context and documenting its nominal eleven-fold increase between 2000 and 2014).

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.
being, and they are conducted within particular “communities of discourse” that happen to exist here and now.\textsuperscript{212} 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 technoliberal beliefs in the power of “trustless trust” and carefully designed code, actual ICO practices do not uphold that ideology.

The disconnect we observe reflects the informality of the ICO world. Paper contracts and IPOs are joint products of law firms, investment banks, regulators, and a panoply of buy-side institutional intermediaries. Smart contracts and ICOs, at least at the moment, largely result from coders and entrepreneurs working at greater distance from risk-averse gatekeepers. Befitting their relatively informal production setting, smart contracts have been ripe for quality control problems. They suffer vast amounts of hacking,\textsuperscript{213} and, as we show, standards as to how code is produced and made legible are wanting.\textsuperscript{214} 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

\textsuperscript{212} See Suchman, supra note 19, at 92.
\textsuperscript{213} See Irrera, supra note 164.
\textsuperscript{214} See supra Part III.
factors, as well as technological ones. 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,” is increasingly 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: 50 2017 ICOs

<table>
<thead>
<tr>
<th>ICO Name</th>
<th>Amount Raised</th>
<th>Industry</th>
<th>ICO Date</th>
<th>Initial Market Value</th>
<th>Market Value 7/31/2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filecoin</td>
<td>$257,000,000</td>
<td>Data Storage</td>
<td>9/10/17</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Tezos</td>
<td>$232,000,000</td>
<td>Infrastructure</td>
<td>7/13/17</td>
<td>$1,209,364,883</td>
<td>$1,171,684,843</td>
</tr>
<tr>
<td>EOS Stage 1</td>
<td>$185,000,000</td>
<td>Infrastructure</td>
<td>7/1/17</td>
<td>$542,468,481</td>
<td>$6,678,854,096</td>
</tr>
<tr>
<td>Paragon</td>
<td>$50,000,000</td>
<td>Drugs &amp; Healthcare</td>
<td>10/15/17</td>
<td>$19,314,902</td>
<td>$8,973,415</td>
</tr>
<tr>
<td>Bancor</td>
<td>$153,000,000</td>
<td>Infrastructure</td>
<td>6/12/17</td>
<td>$94,830,617</td>
<td>$112,542,200</td>
</tr>
<tr>
<td>Kin Kik</td>
<td>$98,000,000</td>
<td>Infrastructure</td>
<td>9/26/17</td>
<td>$82,467,560</td>
<td>$135,236,360</td>
</tr>
<tr>
<td>Status</td>
<td>$100,000,000</td>
<td>Infrastructure</td>
<td>6/20/17</td>
<td>$201,492,471</td>
<td>$213,457,520</td>
</tr>
<tr>
<td>Tron</td>
<td>$70,000,000</td>
<td>Gaming &amp; VR</td>
<td>7/9/17</td>
<td>$29,208,900</td>
<td>$2,399,700,475</td>
</tr>
<tr>
<td>TenX</td>
<td>$80,000,000</td>
<td>Payments</td>
<td>6/24/17</td>
<td>$117,573,375</td>
<td>$93,091,762</td>
</tr>
<tr>
<td>MobileGO</td>
<td>$53,000,000</td>
<td>Gaming &amp; VR</td>
<td>5/25/17</td>
<td>$152,339,600</td>
<td>$10,167,223</td>
</tr>
<tr>
<td>KyberNetwork</td>
<td>$48,960,000</td>
<td>Finance</td>
<td>9/15/17</td>
<td>$255,073,826</td>
<td>$108,701,105</td>
</tr>
<tr>
<td>MCAP</td>
<td>$44,287,318</td>
<td>Trading &amp; Investing</td>
<td>5/7/17</td>
<td>$28,826,424</td>
<td>$273,588</td>
</tr>
<tr>
<td>Loopring</td>
<td>$45,000,000</td>
<td>Trading &amp; Investing</td>
<td>8/16/17</td>
<td>$37,899,054</td>
<td>$137,831,977</td>
</tr>
<tr>
<td>Enigma Catalyst</td>
<td>$45,000,000</td>
<td>Trading &amp; Investing</td>
<td>9/11/17</td>
<td>$53,717,852</td>
<td>$85,471,002</td>
</tr>
<tr>
<td>ICON</td>
<td>$45,000,000</td>
<td>Infrastructure</td>
<td>9/22/17</td>
<td>$1,893,001,514</td>
<td>$458,268,983</td>
</tr>
<tr>
<td>PeerBanks</td>
<td>$42,590,100</td>
<td>Finance</td>
<td>9/22/17</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Electroneum</td>
<td>$40,000,000</td>
<td>Infrastructure</td>
<td>10/20/17</td>
<td>$244,420,733</td>
<td>$81,674,539</td>
</tr>
<tr>
<td>Aeternity</td>
<td>$24,426,689</td>
<td>Infrastructure</td>
<td>6/19/17</td>
<td>$101,036,977</td>
<td>$440,113,497</td>
</tr>
</tbody>
</table>

---

217 We first developed the list of projects from Coinschedule.com. By late summer, 2018, that site no longer provided the relevant data. This chart thus uses a combination of other sources, primarily www.icomarks.com. All data, unless otherwise indicated, came from icomarks.com. Screenshots are on file.

<table>
<thead>
<tr>
<th>Company</th>
<th>Amount Raised</th>
<th>Industry</th>
<th>Start Date</th>
<th>Market Value</th>
<th>Initial Market Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monetha</td>
<td>$37,000,000</td>
<td>Payments</td>
<td>8/31/17</td>
<td>$49,155,179</td>
<td>$7,891,317</td>
</tr>
<tr>
<td>Basic Attention Token</td>
<td>$15,000,000</td>
<td>Commerce &amp; Advertising</td>
<td>5/31/17</td>
<td>$153,729,000</td>
<td>$284,336,885</td>
</tr>
<tr>
<td>Stox</td>
<td>$33,000,000</td>
<td>Trading &amp; Investing</td>
<td>8/4/17</td>
<td>$36,700,152</td>
<td>$10,885,978</td>
</tr>
<tr>
<td>Civic</td>
<td>$33,000,000</td>
<td>Identity &amp; Reputation</td>
<td>6/22/17</td>
<td>$55,657,928</td>
<td>$59,102,197</td>
</tr>
<tr>
<td>Request Network</td>
<td>$32,895,000</td>
<td>Payments</td>
<td>10/17/17</td>
<td>$34,116,439</td>
<td>$42,895,328</td>
</tr>
<tr>
<td>Grid+ (note, added manually)</td>
<td>$32,226,790</td>
<td>Energy &amp; Utilities</td>
<td>12/12/17</td>
<td>$35,698,065</td>
<td>$15,493,393</td>
</tr>
<tr>
<td>ChainLink</td>
<td>$32,000,000</td>
<td>Infrastructure</td>
<td>9/19/17</td>
<td>$54,722,900</td>
<td>$96,571,613</td>
</tr>
<tr>
<td>Polybius</td>
<td>$31,000,000</td>
<td>Finance</td>
<td>6/30/17</td>
<td>$11,114,561</td>
<td>$11,286,714</td>
</tr>
<tr>
<td>Unikoin Gold</td>
<td>$31,400,000</td>
<td>Gambling &amp; Betting</td>
<td>10/23/17</td>
<td>$15,830,700</td>
<td>$12,584,680</td>
</tr>
<tr>
<td>DomRaider</td>
<td>$45,000,000</td>
<td>Payments</td>
<td>10/9/17</td>
<td>$17,002,184</td>
<td>$4,412,625</td>
</tr>
<tr>
<td>Blackmoon Crypto</td>
<td>$30,000,000</td>
<td>Trading &amp; Investing</td>
<td>10/12/17</td>
<td>$29,093,342</td>
<td>$13,403,457</td>
</tr>
<tr>
<td>Bankera PreICO</td>
<td>$29,534,559</td>
<td>Finance</td>
<td>9/19/17</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Blackmoon Crypto</td>
<td>$30,000,000</td>
<td>Data Storage</td>
<td>5/25/17</td>
<td>$21,916,504</td>
<td>$59,096,283</td>
</tr>
<tr>
<td>Storj</td>
<td>$28,000,000</td>
<td>Infrastructure</td>
<td>10/16/17</td>
<td>$22,421,361</td>
<td>$24,142,830</td>
</tr>
<tr>
<td>Monacoc</td>
<td>$26,700,00</td>
<td>Payments</td>
<td>6/18/17</td>
<td>$21,728,700</td>
<td>$109,614,206</td>
</tr>
<tr>
<td>Power Ledger</td>
<td>$13,232,290</td>
<td>Energy &amp; Utilities</td>
<td>10/6/17</td>
<td>$75,432,969</td>
<td>$106,472,515</td>
</tr>
<tr>
<td>Everex</td>
<td>$26,700,000</td>
<td>Finance</td>
<td>8/31/17</td>
<td>$26,737,590</td>
<td>$10,029,365</td>
</tr>
<tr>
<td>Decentraland</td>
<td>$24,000,000</td>
<td>Gaming &amp; VR</td>
<td>8/8/17</td>
<td>$18,092,037</td>
<td>$122,545,988</td>
</tr>
<tr>
<td>FunFair</td>
<td>$20,000,000</td>
<td>Gambling &amp; Betting</td>
<td>6/23/17</td>
<td>$90,924,632</td>
<td>$115,642,649</td>
</tr>
<tr>
<td>Bitclave</td>
<td>$25,500,000</td>
<td>Social Network</td>
<td>11/29/17</td>
<td>$88,293,766</td>
<td>$3,100,377</td>
</tr>
</tbody>
</table>

219 [https://icodrops.com/grid/](https://icodrops.com/grid/) for Amount Raised and ICO Date
220 [https://icodrops.com/chainlink/](https://icodrops.com/chainlink/) for Amount Raised and ICO Date
221 [https://coinmarketcap.com/currencies/unikoin-gold/historical-data/?start=20171120&end=20171125](https://coinmarketcap.com/currencies/unikoin-gold/historical-data/?start=20171120&end=20171125) for Initial Market Value
222 [https://cryptoslate.com/coins/bankera/](https://cryptoslate.com/coins/bankera/) (dollars converted from euros at a 0.846 exchange rate for 9/19/17)
223 [https://icodrops.com/monaco/](https://icodrops.com/monaco/) for Amount Raised and ICO Date; [https://coinmarketcap.com/currencies/monaco/historical-data/?start=20170701&end=20170705](https://coinmarketcap.com/currencies/monaco/historical-data/?start=20170701&end=20170705) for Initial Market Value
<table>
<thead>
<tr>
<th>Company</th>
<th>Initial Capital</th>
<th>Use</th>
<th>Date</th>
<th>Initial Market Value</th>
<th>Current Market Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tierion</td>
<td>$25,000,000</td>
<td>Infrastructure</td>
<td>7/28/17</td>
<td>$71,825,252</td>
<td>$15,166,141</td>
</tr>
<tr>
<td>OmiseGo</td>
<td>$25,000,000</td>
<td>Payments</td>
<td>7/5/17</td>
<td>$46,459,608</td>
<td>$899,402,657</td>
</tr>
<tr>
<td>Aragon</td>
<td>$25,000,000</td>
<td>Infrastructure</td>
<td>5/17/17</td>
<td>$38,864,467</td>
<td>$46,453,168</td>
</tr>
<tr>
<td>0x</td>
<td>$24,000,000</td>
<td>Trading &amp; Investing</td>
<td>9/15/17</td>
<td>$67,035,000</td>
<td>$579,375,044</td>
</tr>
<tr>
<td>Enjin</td>
<td>$23,000,000</td>
<td>Gaming &amp; VR</td>
<td>10/31/17</td>
<td>$22,217,844</td>
<td>$45,939,605</td>
</tr>
<tr>
<td>BlockV</td>
<td>$21,500,000</td>
<td>Infrastructure</td>
<td>10/25/17</td>
<td>$34,409,585</td>
<td>$38,293,702</td>
</tr>
<tr>
<td>FinShi Capital</td>
<td>$21,420,275</td>
<td>Trading &amp; Investing</td>
<td>10/6/17</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>UTRUST</td>
<td>$20,000,000</td>
<td>Payments</td>
<td>11/20/17</td>
<td>$78,017,624</td>
<td>$17,156,284</td>
</tr>
<tr>
<td>Target Coin</td>
<td>$20,711,412</td>
<td>Trading &amp; Investing</td>
<td>8/31/17</td>
<td>$23,542,828</td>
<td>$3,805,577</td>
</tr>
<tr>
<td>ATB Coin</td>
<td>$20,400,000</td>
<td>Infrastructure</td>
<td>9/1/17</td>
<td>$35,927,699</td>
<td>$4,420,874</td>
</tr>
<tr>
<td>Giga Watt224</td>
<td>$15,000,000</td>
<td>Mining</td>
<td>7/31/17</td>
<td>$4,141,800</td>
<td>$2,251,890</td>
</tr>
</tbody>
</table>

## Appendix B: Quotes From Offering Documents About The Three Attributes

<table>
<thead>
<tr>
<th>ICOName</th>
<th>Supply Claims</th>
<th>Burning Claims</th>
<th>Vesting Claims</th>
<th>Modification Claims</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filecoin</strong></td>
<td>Sale Cap: 200,000,000&lt;sup&gt;225&lt;/sup&gt;</td>
<td><strong>Q</strong>: What happens if less than ~200mm tokens are sold? Do they get burnt? If not, who owns them? <strong>A</strong>: This is detailed in the Q&amp;A section of the Sale Economics document. We will split all remaining tokens as follows: 1) We will first apply the remainder to pay for the costs of the token sale itself (many token sales usually pre-allocate this cost) 2) We will sell half of the remainder to the public on network launch. 3) We will keep the other half for market stability (buying and selling filecoin on exchanges to provide market liquidity, price stabilization, correcting unbalanced incentives for storage and retrieval miners, etc.)&lt;sup&gt;226&lt;/sup&gt;</td>
<td>The vesting schedule for each participating group is as follows: Investors: 1 year minimum (advisor pre-sale), 6 month minimum (public sale); Protocol Labs: 6 years, linear vesting; Foundation: 6 years, linear vesting; Miners: Release half-life of 6 years For investors, the following vesting periods and discounts are available: 6 month vesting, 0% discount; 1 year vesting, 7.5% discount; 2 year vesting, 15% discount; 3 year vesting, 20% discount&lt;sup&gt;227&lt;/sup&gt;</td>
<td></td>
</tr>
</tbody>
</table>

| **Tezos** | Following the example set by the Ethereum Foundation, there is no cap on the amount of contributions that will be accepted by the Foundation. This is done in order to ensure that participation is not limited only if two endorsements are made for the same slot or two blocks at the same height by a delegate, this can be denounced. The denunciation would be typically be made by the baker, who includes it as a special 10% to the Foundation, vesting over four years. An amount equivalent to one eighth of the tokens allocated in pools A, B, and C will be allocated to the Foundation. This pool will represent 10% of the total number of tokens issued during the fundraiser...These tokens will vest over a period of 4 years.<sup>228</sup> | If two endorsements are made for the same slot or two blocks at the same height by a delegate, this can be denounced. The denunciation would be typically be made by the baker, who includes it as a special | |

---

<sup>225</sup> Filecoin, Filecoin Token Sale Economics at 3, available at [https://coinlist.co/assets/index/filecoin_index/Filecoin-Sale-Economics-e3f703f8cd5f644aeed7ae3860ce932064ce014dd60de115d67ff1e9047f8a8e.pdf](https://coinlist.co/assets/index/filecoin_index/Filecoin-Sale-Economics-e3f703f8cd5f644aeed7ae3860ce932064ce014dd60de115d67ff1e9047f8a8e.pdf) (last visited June 17, 2018).

<sup>226</sup> Filecoin Investor FAQ, IPFS.IO, available at [https://ipfs.io/ipfs/QmWdXyhqHJWJut5wt4gSCueTjSnFyDHBp3SRfmcqArtz1a/2017-08-08-Filecoin-Investor-FAQ.html](https://ipfs.io/ipfs/QmWdXyhqHJWJut5wt4gSCueTjSnFyDHBp3SRfmcqArtz1a/2017-08-08-Filecoin-Investor-FAQ.html) (last visited August 2, 2018).

<sup>227</sup> Filecoin, Filecoin Token Sale Economics at 5, available at [https://coinlist.co/assets/index/filecoin_index/Filecoin-Sale-Economics-e3f703f8cd5f644aeed7ae3860ce932064ce014dd60de115d67ff1e9047f8a8e.pdf](https://coinlist.co/assets/index/filecoin_index/Filecoin-Sale-Economics-e3f703f8cd5f644aeed7ae3860ce932064ce014dd60de115d67ff1e9047f8a8e.pdf) (last visited June 17, 2018).
to insiders or the “fast-fingered”. The Tezos development team believes that an un-capped fundraiser will promote a widespread distribution of the tokens, a necessary prerequisite to launching a robust network.228

*The Tezos development team believes that an un-capped fundraiser will promote a widespread distribution of the tokens, a necessary prerequisite to launching a robust network.*

<table>
<thead>
<tr>
<th>EOS Stage 1</th>
<th>The EOS.IO software may be configured to enforce a cap on producer awards such that the total annual increase in token supply does not exceed 5%.231 These founders' tokens (“Founders' Tokens”) represent 10% of the aggregate EOS Token Distribution (or 100,000,000 EOS Tokens).232</th>
</tr>
</thead>
</table>

The default EOS.IO Software configuration developed by Block.one locks new founders' tokens distributed pursuant to the launch of an EOSIO Platform in a smart contract and releases 100,000,000 of such tokens (10% of the aggregate EOS Token Distribution) linearly to Block.one every second over a period of 10 years.233

---


| **Paragon** | Paragon will issue a total of 200,000,000 tokens. No additional tokens will ever be generated. Distribution of the initial 100 million tokens will be through a series of token offerings.  

All fees on the Paragon ecosystem will be paid in PRG. The fee structure will keep the price of each transaction low. Each transaction will cost $0.0000005 or 5/1000000000 of a cent (5E-10%). One-half of the fee will be burned each time a transaction occurs, and the other one-half will be deposited to the Paragon Reserve Fund. With the cannabis market surpassing $100B market size in the US alone and current banking issues, we’re hoping to bring a big share of it onto our platform. |
| **Bancor** | **Fixed Price:** 0.01 ETH per 1 BNT (i.e. 100 BNT per 1 ETH)  

**Hidden ETH Cap:** revealed if 80% of the cap is reached.  
  
4.3.1 Implicit burn by transferring tokens to the SmartToken address  
Likelihood: low  
Impact: high  
SmartToken implements functionality that burns tokens if transferred to the address of the token itself. While this seems a sensible default, absent a compelling need for users to be able to burn tokens, we recommend that this functionality be removed, and the token instead throw an exception in this case. User error, and mistakenly entering the token address in the too  

Vesting is a governance practice designed to ensure long-term alignment of interests and is standard for any serious project. All founders and team members will have a 3 year vesting schedule with a 6 month cliff. This means we will mature one-sixth of our tokens every 6 months.  

In order to finance the Kin roadmap, Kik will conduct a token distribution event that will offer for sale one trillion units out of a 10 trillion unit total supply of kin.

The easiest way to understand the Dynamic Ceiling is as a series of ‘hidden hard caps’. A fixed upper limit that restricts further contributions until the next upper limit is revealed. The first ceiling is public and begins the moment 12M CHF (Swiss Francs) equivalent has been reached. It signifies that the Contribution Period will end within 24 hours, or sooner if the hidden hard ceiling has been met. The moment the first ceiling has been triggered there will be a series of additional hidden ceilings that begin after a given number of blocks has been reached. Each hidden ceiling decreases in size and has to be revealed publicly before accepting further contributions.

Each day, once the Rewards Engine is up and running, 0.061% of the remaining reserves will be put into circulation (for a total of 20 percent of remaining reserves every year).

The distribution of SNT created during the contribution period has been outlined by Status’ team in the following way:
- 29% SNT Reserve for future stakeholders, locked for a minimum of a year, to be burned if not deemed necessary for the growth of the network.
- 20% of SNT created during the Contribution Period will be allocated to Status Core Dev; the founders and team, over a 24 month vesting period, with a 6 month cliff. This means Founder tokens will not be immediately tradable.
- 51% of SNT created during the Contribution Period will be allocated to the Status Network token ecosystem.

Based on the work of smart contract developer Jordi Baylina, the Status Network token possesses an interesting attribute - the ability to easily spawn new tokens that have the same balance distribution as the parent token at any given block number. We’re strong believers in a culture of experimentation, and this model preserves fair contribution for early backers, without imposing rigid restrictions on the ability to test new SNT utility as the project evolves over time.

The core team and the Status community are committed to ensuring that the SNT token adds value to the platform and drives network effects. Given the Ethereum ecosystem is still in its infancy and token models are still being researched and developed.

---


238 Nick Johnson, Bancor Audit (no pincite) (May 31, 2017), available at https://gist.github.com/Arachnid/c65fd1bd61a8e0294ae95a4808edc78#file-bancor-audit-md (last visited June 18, 2018).


This allows contributors to continue to participate after the first ceiling has been reached, but reduces the maximum contribution size per ceiling, and solves the problem of run-away 'soft caps'.

<table>
<thead>
<tr>
<th><strong>Tron</strong></th>
<th>TRX is the currency wave field (wave field (TRON)) official tokens, virtual currency and all wave Field (wave field (TRON)) bridge money. A total of 100 billion. 240</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TenX</strong></td>
<td>PAY token price: 1 PAY token equals 1/350 ETH (1 ETH will buy 350 PAY tokens) Total Percentage of all PAY tokens for public, comprising (a) and (b) below: 80% (a) Percentage of all PAY tokens for TenX Initial Token Sale: 51% (b) Percentage of all PAY tokens for community initiatives etc.: 29% Percentage of all PAY tokens for long-term alignment of interests: 20% Target Amount Sold (Fixed limit): 200,000 ETH worth of 10% will be used by TenX to incentivise founders, employees and the development team. Each TenX founder and employee will receive part of their compensation package in PAY tokens, which will vest over 4 years. 240</td>
</tr>
</tbody>
</table>

---


| MobileGO | PAY Tokens\(^{248}\)  
The token has a fixed supply of 100 million tokens, with the full  
supply created on both blockchains.\(^{249}\)  
We will use a percentage of the  
profits from the Gamecredits  
mobile store to buy back and  
burn MobileGo tokens. Once the  
crowdsale is completed, a  
marketing fund will be created  
with a minimum of 50% of funds  
rased. The allocation of these  
resources and the profits that  
these resources generate will be  
audited and made available to  
MobileGo Token holders.\(^{251}\) |
|---|---|
| KyberNetwork | A maximum amount of 226,000,000 KyberNetwork  
Crystal tokens (KNC) will be  
minted.\(^{252}\)  
Before operating, KyberNetwork  
reserves need to pre-purchase  
and store KNC tokens. In every  
trade, a small fraction (exact  
numbers are TBD) of the trade  
volume will be paid by the  
reserve to KyberNetwork  
platform in KNC. This small fee  
represents the reserve’s  
payment in return for the right  
to be able to operate and earn  
profits from trading activities in  
KyberNetwork. The collected  
KNC tokens from the fees, after  
paying for the operation  
The tokens for founders and advisors (around 15% of the total tokens) will be fully vested in 2 years, with a one  
year lock-up period.\(^{254}\) |


expenses and to the supporting partners, will be burned, i.e. taken out of circulation. The burning of tokens could potentially increase the appreciation of the remaining KNC tokens as the total supply in circulation reduces.  

| **MCAP** | There are total of 100 million MCAP tokens.  
 | **Loopring** | Part of providing an open protocol is remaining blockchain agnostic. Hence, Loopring has launched an initial currency on Ethereum (LRC), but it also plans to launch Loopring NEO (LRN) and Loopring QTUM (LRQ)...The total supply of LRN will be 139,507,665.45. This is exactly 1/10 of the total supply of LRC.  
 | **Enigma** | There will now be 150M total tokens in the supply.  
 | **Catalyst** | The crowdsale will continue for 5 days. If we do not sell all 75M tokens in our crowdsale, the unsold tokens will be burned. We will also burn proportional tokens from the remaining supply. This ensures the crowd owns 50% of all created tokens. The team’s ENG tokens vest over multiple years, with all of the team committed to holding their tokens through the first year.  

---

| **ICON** | ICX can be issued up to 20% of total volume annually with the consent of ICON Republic, taking into consideration the ICX trading volume, freezing volume, and transaction fee. However, ICX is not directly issued but by providing nodes with the right to issuance. These rights are granted to the nodes on ICON Republic, and each node is entitled to receive ICX from the ICON Foundation by exercising its rights. Each node may exercise its rights at any time and does not have to exercise immediately.  

Lock up period for team will be 2 years, with vesting 6 months for 4 times. For advisors it varies, but mostly $\frac{1}{8}$ every six months as well. |
|---|---|
| **PeerBanks** | Currently, the total number of IRA tokens is fixed to 1,000,000.  

How many coins is allocated for the devs? - $2000 dollars worth of Electroneum, which is around 20 million coins. Can the devs dump them when the coin gets listed? - No. They cannot sell them within the first 12 months of the launch of the coin. |
| **Electroneum** | With Electroneum’s supply of 21 billion coins we’ve made it easier to mine whole coins and pay with whole coins. |


Aeternity conducted 2 rounds of public token sale. The Aeternity token is named AE... The Aeternity team kept 17% of total supply (46,526,991 AE). This resulted in a total supply of 273,685,830.

Once æternity launches, tokens will exist on æternity. However even if æternity did exist, it wouldn’t give us the ability to do a decentralized token sale—Ethereum is great for this type of use-cases, that require a fully public index of things (e.g. tokens, ...). æternity is focusing on scalable, real-world uses-cases.

Monetha

The creation will be capped (“Soft Cap”) upon receipt of ETH equivalent to EUR 7m (fixed on 28000 ETH). This amount is subject to change before the Token Creation event. The Token Creation period will last 31 (thirty one) days, if Soft Cap is not reached sooner. If the Soft Cap is reached before the end of 31 (thirty one) days, additional contributions will be accepted for 120 hours in case some contributors missed the very short window for MTH creation.

Tokens that are not sold during the Crowdsale will be burned automatically by the smart contract.

% of tokens generated to Monetha team: 15%. Automatically locked for 12 months by smart contract.

% of tokens generated for loyalty program: 13%. Automatically locked for 12 months by smart contract.

% of tokens generated to bounty campaign, advisors, partners, ICO campaign costs: 12%

% of tokens generated for future company financing: 10%. Automatically locked for 12 months by smart contract.

---


266 Note: Aeternity has discussed “burning” its tokens on the Ethereum blockchain in the process of converting the tokens to currency on the Aeternity blockchain, which does not yet exist, as in the comment by the official account in this thread: https://www.reddit.com/r/Aeternity/comments/6za07b/burning_token/


### Basic Attention Token

Token Distribution
Brave: 13.3% of max; 200 million
BAT. User growth pool: 300 million BAT. Token available to public at launch: 1 billion (corresponding to the ETH raised at token launch).

BAT Total 133,650,000 (180 Day Lockup): Development Pool

#### Stox

In order to finance Stox’s roadmap, Stox will conduct a token sale of an initial supply of STX tokens. STX will be sold at a constant price (in ETH) and the initial supply will depend on amount of STX sold. As of the conclusion of the sale, the distributed STX will constitute the entirety of the available liquid supply. A portion of the supply would be preallocated to invest.com as the founding member of the ecosystem, in a long term vesting schedule. Major portion of the allocation to Stox Ltd. will be used for bringing further strategic partners to the Stox platform.

<table>
<thead>
<tr>
<th>% of Total Supply</th>
<th>Beneficiary Special terms</th>
<th>Beneficiary Special terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>Token sale participants</td>
<td>Uniform 12-month vesting schedule</td>
</tr>
<tr>
<td>12.5%</td>
<td>invest.com Ltd.</td>
<td>Uniform 12-month vesting schedule</td>
</tr>
<tr>
<td>10%</td>
<td>Stox team</td>
<td>Uniform 24-month vesting schedule</td>
</tr>
<tr>
<td>27.5%</td>
<td>Stox Ltd.</td>
<td>Will be used to bring strategic partners to the Stox ecosystem, and as operational reserve</td>
</tr>
</tbody>
</table>

---


272 Basic Attention Token, FAQ (no pincite), available at [https://basicattentiontoken.org/faq/](https://basicattentiontoken.org/faq/) (last visited June 20, 2018).


**Civic**

Company will create 1 billion Tokens to be allocated as follows: 275

(i) One third of the Company Inventory will remain in a locked state for 1 year from the Crowdsale End Date; another third of the Company Inventory will remain in a locked state for 2 years from the Crowdsale End Date; and the remaining third of the Company Inventory will remain in a locked state for 3 years from the Crowdsale End Date. (ii) Once unlocked, Company reserves the right to use the Company Inventory for any purposes at its sole discretion. (iii) In no event will the Company sell any Tokens from the Company Inventory before the date that is one year after the Crowdsale End Date. (iv) In no event will any Tokens from the Company Inventory be sold by the Company at any point for a Price Per Token of less than USD $0.10. 276

---

**Request Network**

The Request Network token launch ended successfully with 100% of the tokens distributed. We are glad to have received positive feedbacks from the community and that the event happened in a smooth way. The fundraising was capped at 100,000 ETH for 500,000,000 REQ and we limited the number of approved registrants at 14,885. 277

This layer is chargeable, in that each extension will take a fee that will be partially burned and partially transferred to the extension developers, with the extensions accrued on the same invoice. Costs decrease over time to remain competitive and discourage alternative systems. The costs of these extensions is estimated to be between 0.1% and 0.5% initially, though as the system grows, the costs will be reduced. More than 5,000 billion dollars in payments are made each day, and in the end it will be enough to finance the network by less than 0.1%. 278

---

**Grid+**

A fixed number of GRID tokens (300,000,000) will be minted before the upcoming token sale - this will be the only time GRID are created. 279

Each GRID token will be a credit on the Grid+ platform, redeemable by customers of the Grid+ platform for the right to purchase 500 kWh of electricity at the wholesale price available.

20% (60,000,000) will be held by the founders of Grid+; of these, 25% will remain time-locked for each of 6, 12, and 18 months, with the final 25% also being unlocked after 18 months. Another 20% (60,000,000) will be held by external owners of Grid+; these will be time-locked on the same schedule and in the same percentages as the founders’ tokens. 280

---

---


to Grid+ in the relevant jurisdiction at the time such electricity is received by the redeeming customer. At the time of redemption, GRID tokens will be assigned a timestamp by the redemption contract and taken out of supply forever via a mechanism modeled after EIP 661.\footnote{Grid+, Grid+ Whitepaper at 40, available at \url{https://gridplus.io/assets/Gridwhitepaper.pdf} (last visited June 24, 2018).}

**ChainLink**
The total supply of the token is 1,000,000,000, and each token is divisible up to 18 decimal places.\footnote{Grid+, Grid+ Whitepaper at 40, available at \url{https://gridplus.io/assets/Gridwhitepaper.pdf} (last visited June 24, 2018).}

To prevent accidental burns, the token does not allow transfers to the contract itself and to 0x0.\footnote{Steve Ellis, LINK Token Contracts (no pincite) (Mar. 13, 2018), available at \url{https://github.com/SmartContractKit/LinkToken} (last visited June 24, 2018).}

**Polybius**
The total supply is not locked, as we will need to be able to add tokens before the end of sale and revoke the unsold amount... At the end of the crowdsale all sold tokens are considered to be 93% of the total supply. The remaining 7% are then distributed among founders and bounties receivers according to the information above.\footnote{Steve Ellis, LINK Token Contracts (no pincite) (Mar. 13, 2018), available at \url{https://github.com/SmartContractKit/LinkToken} (last visited June 24, 2018).}

Company will create a total of 1,000,000,000 UnikoinGold by the time of the Delivery Date (defined in Section 5 below). No additional UnikoinGold will be

See discussion in text

See discussion in text

See discussion in text

\footnote{Polybius, Polybius Prospectus at 3, 5 (June 8, 2018), available at \url{https://polybius.io/media/prospectus.pdf} (last visited June 24, 2018).}
| **DomRaider** | created. The Trading Operation foresees the creation and distribution of 1 billion DomRaider Tokens (DRT) distributed as follows. | Sold tokens may be used and transferred from the time they are assigned. 20% of tokens distributed free of charge to stakeholders that have contributed to the operation’s success will be immediately useable and transferable. The remaining 80% will be released gradually at 10% of the total each month from the date the first tokens are issued. In this way, every holder of tokens obtained through this category will have received full use and transferability of these tokens 8 months following their issue. The tokens held in reserve by DomRaider will be locked at a level of 90% of the reserve and released gradually at 5% of the total reserve per month. |
| **Blackmoon Crypto** | All available BMC will be issued during the Distribution period. This will be a one-time operation and no additional issuance is available for BMC tokens. The total number of BMC to be issued will be calculated at the end of the Distribution Period according to the formula: amount of BMC sold during the Distribution multiplied by 2. 50% of the proceeds are distributed among the fund’s token holders via a buy-back process. In this way, distribution of income provides liquidity of the fund’s tokens. Bought-out tokens are burned so that income will continue to increase for the remaining fund tokens. 30% of the BMCs will be allocated to the Company reserve and locked for a minimum of 36 months. This reserve is a necessary foundation for sustainable future development of the Blackmoon Crypto Platform. 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. Some BMCs from this pool (but not more than 5% of all BMCs) will be allocated to non-operational advisors and will be locked with a six-month cliff without vesting. Up to 3% will go to subcontractors and bounty campaign members without vesting. |
| **Banhera PreICO** | The hard cap (how many tokens will be issued) will be | The 25% of tokens will be attributed to the team as a motivation as well as for bounty program for outsiders. The team part of tokens will be allocated over time. |

---


determined by dividing a number of tokens issued during pre-ICO by 0.1... Hence, the total HARDCAP for pre-ICO and ICO is 10,000,000,000 BNK (2,500,000,000 + 7,500,000,000) worth 177M EUR (25M EUR + 152M EUR) and at least 750M EUR for the SCO. 291

Agrello
With a total of 150 million DLT token (and no plan to create new), Agrello’s team has decided to distribute 90 million DLT via its ICO which will take place on July 10th, 2017 till August 9th, 2017 (token distribution date as well), with a minimum investment goal of 4,000 BTC. 292

The token sale funds are held in thousands of cold stored addresses. This is a way that the sale was conducted and anyone associated with the sale would know this. Agrello is a private company and we plan on having open dialogue with our supporters and we have been very appropriately been using funds. There are not 1 or a few addresses that show the funds collected. No one on the team, any contractors, advisors, or partners have received DLT. All parties have vesting periods for their tokens. You can see the Delta balances here: https://etherscan.io/token/0x07e3c70653548b04f0a75970c1f81b4cbbfb6066#balances

Storj
At present, the total supply of Pre-existing Tokens is 500 million, 51,173,144 of which are in Pre-existing Tokens in circulation ("Circulating Pre-existing Tokens"). As of April 1, 2017, Storj U.S. held 448,967,875 Pre-existing Tokens ("Storj U.S. Pre-existing Tokens"). 293

The Company anticipates selling approximately 75 million Tokens during the Sale Period. The Tokens to be sold during the Sale Period will be from a pool of Company-owned Tokens transferred from the Company Custodial Wallet to the Smart Contract System. All Tokens will be of equal value and functionality. During the Sale Period, Company will burn Tokens not sold or burned during the Sale Period will be retained by the Company (the "Retained Tokens"). At least 80% of Retained Tokens retained will be placed into time-locked smart contracts and remain in a locked state for at least six (6) months. Although it has no plans to do so at this time, the Company reserves the right to burn Retained Tokens at any point during or after the Sale Period. Over time, the Company currently anticipates using the Retained Tokens to compensate employees (including salaries and non-salary compensation), to fund future development of Storj and the Network, provide grants to (or purchase equity stakes in) third-parties working on projects in the Storj ecosystem, donate Tokens to non-profit entities, and support general development of the Storj ecosystem. These anticipated purposes are listed for illustration only, and Company reserves the right to use Reserved Tokens for these purposes (or others) at its sole discretion. 294


least one Token in the Company Custodial Wallet for each Token it sell. . . . Although it has no plans to do so at this time, the Company reserves the right to burn Retained Tokens at any point during or after the Sale Period.296

Eidoo

<table>
<thead>
<tr>
<th>Total number of token: 100 million298</th>
<th>Unsold tokens during the sale will be burned.298</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Eidoo Tokens293</th>
<th>Total (millions of tokens)</th>
<th>Unlocked (millions of tokens)</th>
<th>Locked (millions of tokens)</th>
<th>Lock Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eidoo</td>
<td>47</td>
<td>0</td>
<td>47</td>
<td>20M EDO</td>
</tr>
<tr>
<td>Founders</td>
<td>13</td>
<td>3</td>
<td>10</td>
<td>15M EDO</td>
</tr>
<tr>
<td>Advisors</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>6M EDO</td>
</tr>
<tr>
<td>Early Investors</td>
<td>12</td>
<td>3,6</td>
<td>8,4</td>
<td>2 years</td>
</tr>
<tr>
<td>Pre-sale</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>4m EDO</td>
</tr>
<tr>
<td>Token Sale</td>
<td>20</td>
<td>20</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Unsold tokens during the sale will be burned.298


Monaco

Monaco Card aims to accept up to 150,000ETH from our initial token partners and create approximately 17.6m MCO for sale in exchange for the ETH committed. The MCO smart contract will stop accepting commitments at 888,888ETH hard cap. The

At any time, a holder of MCO can “Redeem and Burn” the MCO for their pro-rata share of each token held by the MCO Asset Contract. The holder will irrevocably destroy the MCO, and in exchange, the MCO Asset Contract will transfer the underlying tokens to the holder.

We are setting aside 30% of all MCO created as Reserve Tokens. These MCO will not be issued or sold during the initial sale and are locked in a smart contract. If at some point it seems advisable for the Monaco Card project to sell more tokens, some or all of these may be offered in an auction format or some other format that suits the capital needs of the project.

Specifically, there are substantial balance sheet strength requirements in case Monaco decides to apply for a full banking license in the European Union or Asia. In the interim, these MCO will not be used in any way. They will not be considered as issued for Redeem and Burn calculations.

It is possible these MCO will never be issued, however, we feel it is prudent to have some backup if needed. In any event, Monaco will engage directly with MCO holders to seek guidance and market reaction before any of

Token Sale will last for 30 days. If soft-cap is reached, the event will be extended for 7 days and then closed. If hard-cap is reached, the event will close automatically.

We are setting aside 30% of all MCO created as Reserve Tokens. These MCO will not be issued or sold during the initial sale and are locked in a smart contract.

MCO token will have a market value at or above the assets contained in the MCO Asset Contract. If the value goes below, market participants will be incentivized to purchase MCO and burn it; this will then push the value of MCO back up.

Power Ledger

1,000,000,000 POWR tokens have been created and the total amount of tokens will be allocated as follows:

- Q: Are there any plans to burn the remaining tokens held by PL if they are not needed for future funding?
  - A: We will need them if we grow to the size aimed for that was the logic in 1 b selection. But like the thinking!

The POWR tokens which are gifted to or discounted to Application Hosts, from the Growth Pool, will be held in escrow for a minimum period of 1-3 years after they are distributed to ensure that they are used on the Platform.

A further 250,000,000 tokens will be retained for any future funding needs of Power Ledger and the Platform, including development or on-boarding future Participants if required. Due to the dependency on the outcome of the Token Sale, this allocation will be held in the Power Ledger Escrow. The escrow period will be 2 years. The escrow period in respect of these tokens will commence at the date of distribution.

The Developer's and Founder's tokens will be distributed to Power Ledger’s directors, employees and contractors engaged in the building of the Platform. All of the Developer's and Founder's tokens will be subject to escrow for a period of between six and 18 months, with their release linked to performance variables. The escrow period in respect of these tokens will commence at the completion of the Token Sale.

EVX Vesting Schedule

Team holdings: 15%
- not vested 5%

EVX Tokens supply: approx. 25,000,000* Tokens offered for a public sale: If less than 70,000 ETH in proceeds has been received by the termination of the Sale

---


---

Electronic copy available at: https://ssrn.com/abstract=3215345
Decentraland

<table>
<thead>
<tr>
<th>Period (the “Minimum Threshold”), the unsold balance of Tokens that is authorized but unissued to purchasers will be retained in Company inventory to be utilized by Company as part of its incentive Development Fund to be distributed in accordance with the decision of the board on a quarterly basis as elsewhere set forth herein. 307</th>
</tr>
</thead>
<tbody>
<tr>
<td>No tokens are pre-issued before the crowdsale event. 307</td>
</tr>
<tr>
<td>The final number of tokens is defined after the end of the token sale based on amounts contributed.</td>
</tr>
<tr>
<td>Decentraland will use an Ethereum smart contract to maintain a ledger of ownership for land parcels in the virtual world. We call these non-fungible digital assets LAND. LAND is bought by burning MANA, a fungible ERC20 token of fixed supply. This token serves as a proxy for the cost of claiming a new parcel. The LAND contract uses a burn function to destroy MANA and create a new entry in the LAND registry. New parcels need to be adjacent to a non-empty parcel. 310</td>
</tr>
<tr>
<td>Increasing Sale: MANA tokens will sell at a price that goes from $24 USD per LAND equivalent to $40 USD. A hard cap is set at $25 million USD. The distribution of additional tokens is fixed. Inflation rate: Included is an 8 percent increase of the token supply for the first year, and a lower rate in subsequent years. This is implemented through a Continuous Token Model. This structure will allow Decentraland to regularly expand while accommodating new users. 309</td>
</tr>
<tr>
<td>20 percent will go to the development team, early contributors and advisors, and the remaining 20 percent will be held by the Decentraland Foundation. Founders will have three-year vesting. 312</td>
</tr>
</tbody>
</table>

The Phase 1 creation crediting period will end no later than July 7, 2017 at 14:00 UTC. If 500 million (500,000,000) FUN have been created at any time before Jul 7, 2017 14:00 UTC, token creation will continue for 4 additional hours at that time. After 4 hours or 1 billion FUN are issued, the crediting period will cease, the receiving contract will be marked “finished” and it will reject Ether from that time on by calling throw. As soon as Phase 1 closes, additional tokens will be created in an amount equal to three times the amount sold during the Phase 1 creation crediting period and held in trust until the Phase 2 token issuance event. At some point following the Phase 1 close, the Phase 2 token issuance event will begin. In Phase 2, all tokens held in trust will be offered in a Dutch auction. Whatever tokens remain unsold in this event will be distributed pro rata to holders of tokens sold in Phase 1 issuance.

The Token Contract implements the ERC20 standard with a few additional features. The contract is split into three separate parts: A “Ledger” contract referred to by the “Controller”–this contract holds all balances and manages all minting and burning and will not change except in extreme circumstances.

Founder Stake: FunFair developers, founders and angel investors will receive 37.5% of total tokens, released slowly over an 18-month period. Advisor Stake: FunFair advisors will receive 2.5% of total tokens, released immediately.

## Bitclave

<table>
<thead>
<tr>
<th>General Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer Activity Token (CAT)</td>
</tr>
<tr>
<td>2 billion total token supply</td>
</tr>
<tr>
<td>550,842,000 tokens distributed in token sale or 25,547,000 USD hard cap 217</td>
</tr>
</tbody>
</table>

| Team has vesting for 2 years. They cannot sell the tokens 218 |

<table>
<thead>
<tr>
<th>Tierion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tierion is creating a total supply of 1 billion (1,000,000,000) TNT tokens, of which: 35% will be available for purchase as described above, 29% will remain in the Company's inventory under a lock up, 35% will be allocated to incentivize the Tierion ecosystem, and 1% will be used to cover token sale costs. 220</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Will there be a lock-up on tokens retained by Tierion?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, these tokens will be locked up for six months. After the initial lockup, they will be distributed 10% per quarter for ten consecutive quarters. 221</td>
</tr>
</tbody>
</table>

## OmiseGo

<table>
<thead>
<tr>
<th>During the crowdsale period (&quot;OMG token creation period&quot;), up to a total of USD $25 million (Maximal Launch Quantity) equivalent of OMG are to be created by the smart contract, all equal value and functionality, but divided by the smart contract itself acts as a bond for its activity on this blockchain, improper activity results in the token/bond being burned on the OMG chain. By creating a custom chain with deep enforcement, we are able to construct a system where</th>
</tr>
</thead>
<tbody>
<tr>
<td>(iii) OmiseGO reserve [20% of OMG issued]</td>
</tr>
<tr>
<td>Directly released by the smart contract to OmiseGO for future costs and uses including use for network validation as part of the development and execution of the project. These OMG are locked through a smart contract function and may not be transacted by OmiseGO for a period of 1 year, starting at the end of the creation period.</td>
</tr>
<tr>
<td>(iv) Team [9.9% of OMG issued]</td>
</tr>
<tr>
<td>Reserved for team members and key contributors who worked to develop the ideas, supporting structures, and actual implementations of the OmiseGO Project. These OMG are locked for 1 year. 224</td>
</tr>
</tbody>
</table>

| OMG will be a standard Ethereum ERC20 token, until the OmiseGO chain ("OMGchain") is launched. When OMGchain is launched, ERC20-OMG is used as a Proof-of-Stake token on this network. This is achieved by |

### References


<table>
<thead>
<tr>
<th><strong>Aragon</strong></th>
<th><strong>OmiseGo</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>contract in</strong></td>
<td><strong>consensus rules optimize for</strong></td>
</tr>
<tr>
<td><strong>to different pools, for</strong></td>
<td><strong>high-performant activity.</strong></td>
</tr>
<tr>
<td><strong>both public and private</strong></td>
<td><strong>allocating control of one’s the</strong></td>
</tr>
<tr>
<td><strong>distribution:</strong></td>
<td><strong>ERC20 to an ETH contract</strong></td>
</tr>
<tr>
<td><strong>Public</strong></td>
<td><strong>reflecting the OMG chain.</strong></td>
</tr>
<tr>
<td>(i) Sale (65.1% of OMG issued)</td>
<td><strong>Further improvements are</strong></td>
</tr>
<tr>
<td>The bulk of the OMG will be</td>
<td><strong>possible from reallocation of</strong></td>
</tr>
<tr>
<td>released in a sale, where they</td>
<td><strong>ERC20 tokens and may be</strong></td>
</tr>
<tr>
<td>will be sold in exchange for up to</td>
<td><strong>taken if it proves to be a better</strong></td>
</tr>
<tr>
<td>a maximum of USD $25 million</td>
<td><strong>design, but the current</strong></td>
</tr>
<tr>
<td>equivalent.</td>
<td><strong>approach is to have the ERC20</strong></td>
</tr>
<tr>
<td></td>
<td><strong>token locked into activity on a</strong></td>
</tr>
<tr>
<td></td>
<td><strong>contract on the ETH chain. It</strong></td>
</tr>
<tr>
<td></td>
<td><strong>is the responsibility of the</strong></td>
</tr>
<tr>
<td></td>
<td><strong>community to elect to allocate</strong></td>
</tr>
<tr>
<td></td>
<td><strong>the ERC20 token towards the</strong></td>
</tr>
<tr>
<td></td>
<td><strong>OMG chain, as the community</strong></td>
</tr>
<tr>
<td></td>
<td><strong>has control over the network.</strong></td>
</tr>
<tr>
<td><strong>Aragon</strong></td>
<td><strong>70/15/15 distribution: 70% will</strong></td>
</tr>
<tr>
<td></td>
<td><strong>go to purchasers, 15% to the</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Foundation, and 15% to the</strong></td>
</tr>
<tr>
<td></td>
<td><strong>founders and early contributors</strong></td>
</tr>
<tr>
<td></td>
<td><strong>who have worked on the</strong></td>
</tr>
<tr>
<td></td>
<td><strong>project...</strong></td>
</tr>
<tr>
<td></td>
<td><strong>We want our token sale to last so</strong></td>
</tr>
<tr>
<td></td>
<td><strong>we can onboard to our</strong></td>
</tr>
<tr>
<td></td>
<td><strong>community as much people as we</strong></td>
</tr>
<tr>
<td></td>
<td><strong>can. So uncapped was the</strong></td>
</tr>
<tr>
<td></td>
<td><strong>obvious choice.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>But since we don’t want another</strong></td>
</tr>
<tr>
<td></td>
<td><strong>The DAO scenario to happen, a</strong></td>
</tr>
<tr>
<td></td>
<td><strong>security cap is a must.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>So we will place a hidden cap.</strong></td>
</tr>
<tr>
<td><strong>70/15/15 distribution: 70% will</strong></td>
<td><strong>70/15/15 distribution: 70% will go to purchasers, 15% to the Foundation, and 15% to the founders and early contributors who have worked on the project. The founder and early contributors will all have vesting.</strong></td>
</tr>
<tr>
<td><strong>go to purchasers, 15% to the</strong></td>
<td><strong>Aragon Network Token (ANT) will initially begin as an</strong></td>
</tr>
<tr>
<td><strong>Foundation, and 15% to the</strong></td>
<td><strong>upgradable token, but will</strong></td>
</tr>
<tr>
<td><strong>founders and early contributors</strong></td>
<td><strong>evolve to serve as the</strong></td>
</tr>
<tr>
<td><strong>who have worked on the</strong></td>
<td><strong>governance token for the</strong></td>
</tr>
<tr>
<td><strong>project...</strong></td>
<td><strong>Aragon Network when</strong></td>
</tr>
<tr>
<td><strong>We want our token sale to last so</strong></td>
<td><strong>deployed...</strong></td>
</tr>
<tr>
<td><strong>we can onboard to our</strong></td>
<td><strong>In terms of architecture, the</strong></td>
</tr>
<tr>
<td><strong>community as much people as we</strong></td>
<td><strong>Aragon Token has a controller</strong></td>
</tr>
<tr>
<td><strong>can. So uncapped was the</strong></td>
<td><strong>which can manage its critical</strong></td>
</tr>
<tr>
<td><strong>obvious choice.</strong></td>
<td><strong>functionality (for example,</strong></td>
</tr>
<tr>
<td><strong>But since we don’t want another</strong></td>
<td><strong>minting new tokens). During</strong></td>
</tr>
<tr>
<td><strong>The DAO scenario to happen, a</strong></td>
<td><strong>the sale period, the smart</strong></td>
</tr>
<tr>
<td><strong>security cap is a must.</strong></td>
<td><strong>contract running the sale</strong></td>
</tr>
<tr>
<td><strong>So we will place a hidden cap.</strong></td>
<td><strong>serves as the token controller.</strong></td>
</tr>
</tbody>
</table>

The cap will be cryptographically sealed, and revealed after the sale. If it's reached, we will issue an emergency stop that will stop the acceptance of new purchases. Since we take security seriously, we will also set a hardcoded cap into the sale contract, just in case.326

ANT will continue to be minted by the network following the initial sale and network deployment. Minting new tokens will have a cost, and a percentage of the fees (decided by governance) paid by organizations to join the network will fund the minting of new tokens. This creates an incentive for Aragon organizations to pay fees, as organizations that contribute more will receive more ANT. This means that the organization will be more influential in network decisions. The cost to mint new tokens will be determined by ANT token holders. This will likely be a contentious decision, and one where the basic economic principles of supply and demand need to be considered. For example, consider the scenario where the cost of minting tokens

Once the sale is complete, a placeholder contract will take over as controller (does not perform any critical functions). The placeholder controller will transfer controller power to the full Aragon Network after deployment. The Aragon developers core group will deploy the Aragon Network's code when appropriate and the token will serve as a governance mechanism.329

is too low. More and more tokens will be added to the supply, until supply greatly outweighs demand. This is a recipe for inflation and the value of individual ANT tokens will fall. Ultimately, we believe that token holders will eventually decide on a healthy equilibrium for inflation. By weighing the opinion of every stakeholder, the market will accurately reflect the optimal minting cost.


The total number of tokens released during both the main sale and pre-sale events will add up to 35% of the total supply of $V. During the main sale event, 1 billion $V will be released for sale to the public. The sale will continue for 5 days, with a hard cap of $20 million. The final price per token will depend on the total sum raised in the main sale, with a maximum price of $0.02 per token.

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

The amount of issued tokens will depend on the sum raised in dollars according to the rate 1 USD = 1 token.

Minimum capital – $30 000 000.
Minimum sum of the issued tokens = 30 000 000.
Maximum Capital - $50 000 000.
Maximum sum of the issued tokens = 50 000 000.

15% of the tokens will be locked up long term. To ensure long-term success of our project, this portion of the tokens will be locked up for 6 years with some vesting starting at year 3. We have absolute confidence in our project and are fully dedicated to the spread vAtoms throughout the world and having this reserve will be the best way to add further fuel to this vision in the future.

25% of the tokens will be reserved for incentives to promote the use of BLOCKv and vAtoms. These tokens will be used to reward developers for devising innovative uses for vAtoms, and to reward vAtom end-users for performing specific actions. The diving goal is to proliferate the use of vAtoms all over the world and across many industries. These tokens will be locked up for 2 years, with 1/5th being available after the token sale and 1/5th being unlocked every 6 months thereafter to ensure regular and timely incentives.

25% of the tokens will be held by the company with a portion going to the development team, early contributors and advisors over time. We believe that rewarding our supporters appropriately will ultimately contribute to our project’s success in the long-term. These tokens will be locked up for 2 years, with 1/5th being available after the token sale and 1/5th being unlocked to the company every 6 months thereafter.


| UTRUST | Token Pool Supply: 500,000,000 (five hundred million)...
| | Total Token Pool: 1 billion
| | How will this strategic value coupling work? Each time a buyer pays with any cryptocurrency via the UTRUST payment platform a percentage of the transactional fee will be used to buyback UTK and to remove them from the market. The removed tokens will be burned. This will reduce the amount of UTK supply further driving demand, the adoption of the platform and the value for contributors. The amount of UTK was projected to be reduced from the initial 1 billion to a minimum cap of 100 million, at a rate no faster than 50 million a year.
| 50m: UTRUST
| Target Coin | TGT Coin plans to issue 2 Bn coins. 1.34 Bn coins are available to the public and 260 Mn coins are held by the management team and 400 Mn coins are held by the pre-ICO investors.
| | At the beginning the tokens will not have any features. The use as a means of payment will only be possible after the regulatory status of the UTRUST platform has been clarified with FINMA.
| | 50m: PRE-SALE
| | 100m: PRIVATE INVESTORS (1 year vesting)
| **ATB Coin** | As a POS cryptocurrency, ATB Coin will start with an open ICO. During the ICO anyone will be able to purchase ATB Coin tokens and also can receive a certain number of ATB Coins as a bonus. The total number of coins that are offered to the public during the ICO equals a number of coins in the genesis block, which is 50 000 000 ATB.  
| **Giga Watt** | If a cap of 30,000,000 WTT tokens sold is reached before the scheduled end of the Token Launch, Cryptonomos at its own discretion may issue WTT tokens ahead of the specified date to provide access to the facilities built by that time.  
347 Giga Watt, Giga Watt White Paper at 16 (May 2017), available at https://wtt.cryptonomos.com/white-paper.pdf (last visited June 26, 2018). | WTT tokens retained for distribution to the team will be distributed only when no proceeds from over-subscribed tokens remain in escrow awaiting the completion of additional processing center capacity construction. WTT tokens retained for distribution to partners and advisors will be distributed on a case by case basis.  
Appendix C: Summary of Code/Contract Audit
*If you believe there is an error in this chart, please contact the authors explaining why and if we agree, we will make a prompt correction*

<table>
<thead>
<tr>
<th>ICOName</th>
<th>Scarcity Claimed (Y/N)</th>
<th>Scarcity Coded (Y/N)</th>
<th>Vesting Claimed (Y/N)</th>
<th>Vesting Coded (Y/N)</th>
<th>Burning Claimed (Y/N)</th>
<th>Burning Coded (Y/N)</th>
<th>Modification Disclosed (Y/N)</th>
<th>Modification Coded (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filecoin</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Tezos</td>
<td>ScarcityNN</td>
<td>VestingYN</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>EOS Stage 1</td>
<td>ScarcityNN</td>
<td>VestingYN</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Paragon</td>
<td>ScarcityYY</td>
<td>VestingYN</td>
<td>BurnningYY</td>
<td>BurnningYY</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Bancor</td>
<td>ScarcityYY</td>
<td>VestingYN</td>
<td>BurnningYY</td>
<td>BurnningYY</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Kin Kik</td>
<td>ScarcityYY</td>
<td>VestingYY</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Status</td>
<td>ScarcityYN</td>
<td>VestingYY</td>
<td>BurnningYY</td>
<td>BurnningYY</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationYY</td>
<td>N/A</td>
</tr>
<tr>
<td>Tron</td>
<td>ScarcityYY</td>
<td>VestingYN</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>TenX</td>
<td>ScarcityYN</td>
<td>VestingYN</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>MobileGO</td>
<td>ScarcityYY</td>
<td>VestingNN</td>
<td>BurnningYY</td>
<td>BurnningYY</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>KyberNetwork</td>
<td>ScarcityYY</td>
<td>VestingYN</td>
<td>BurnningYN</td>
<td>BurnningYN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>MCAP</td>
<td>ScarcityYY</td>
<td>VestingNN</td>
<td>BurnningNY</td>
<td>BurnningNY</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Loopring</td>
<td>ScarcityYY</td>
<td>VestingYN</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Enigma Catalyst</td>
<td>ScarcityYY</td>
<td>VestingYN</td>
<td>BurnningYY</td>
<td>BurnningYY</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>ICON</td>
<td>ScarcityNY</td>
<td>VestingYN</td>
<td>BurnningNY</td>
<td>BurnningNY</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>PeerBanks</td>
<td>ScarcityYY</td>
<td>VestingNN</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Electroneum</td>
<td>ScarcityYN</td>
<td>VestingYN(^{351})</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Aeternity</td>
<td>ScarcityYY</td>
<td>VestingYN</td>
<td>BurnningYN</td>
<td>BurnningYN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Monetha</td>
<td>ScarcityYY</td>
<td>VestingYN</td>
<td>BurnningYN</td>
<td>BurnningYN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Basic Attention Token</td>
<td>ScarcityYY</td>
<td>VestingYY(^{352})</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Stox</td>
<td>ScarcityYY</td>
<td>VestingYY</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNY</td>
<td>N/A</td>
</tr>
<tr>
<td>Civic</td>
<td>ScarcityYY</td>
<td>VestingYN</td>
<td>BurnningNN</td>
<td>BurnningNN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Request Network</td>
<td>ScarcityYY</td>
<td>VestingNY</td>
<td>BurnningYN</td>
<td>BurnningYN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
<tr>
<td>Grid+</td>
<td>ScarcityYY</td>
<td>VestingYY</td>
<td>BurnningYN</td>
<td>BurnningYN</td>
<td>N/A</td>
<td>N/A</td>
<td>ModificationNN</td>
<td>N/A</td>
</tr>
</tbody>
</table>

\(^{350}\) An early draft made claims about the Filecoin code based on an Etherscan token that appeared to be associated with the project. [https://etherscan.io/address/0xc52f51ceacb229f2be90a3f662a3d8a0e425316a#code](https://etherscan.io/address/0xc52f51ceacb229f2be90a3f662a3d8a0e425316a#code). However, the Filecoin General Counsel, Marvin Ammori, assured us that that code was not associated with Filecoin.

\(^{351}\) An early draft listed Electroneum as NN for vesting. But we found, per Appendix B, an answer in a FAQ that pre-dated the ICO, which claimed a prohibition on sale within 12 months. See [https://etherscan.io/address/0x67fa2e06c9c6d4332f330e14a66bdf1873ef3d2b#code](https://etherscan.io/address/0x67fa2e06c9c6d4332f330e14a66bdf1873ef3d2b#code).

\(^{352}\) An early draft listed BAT as YN for vesting because its main smart contract did not contain vesting code. However, a secondary contract, to which tokens were transferred before the ICO, did contain vesting code. See [https://etherscan.io/address/0x67fa2e06c9c6d4332f330e14a66bdf1873ef3d2b#code](https://etherscan.io/address/0x67fa2e06c9c6d4332f330e14a66bdf1873ef3d2b#code).
<table>
<thead>
<tr>
<th>Company</th>
<th>Scarcity</th>
<th>Vesting</th>
<th>Burning</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChainLink</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Polybius</td>
<td>Unauditable</td>
<td>Unauditable</td>
<td>Unauditable</td>
<td>ModificationYY</td>
</tr>
<tr>
<td>Unikoin Gold</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>DomRaider</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Blackmoon Crypto</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Bankera Pre0ICO</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Agrello</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Storj</td>
<td>YY</td>
<td>NN</td>
<td>YY</td>
<td>YY</td>
</tr>
<tr>
<td>Eidoo</td>
<td>YY</td>
<td>NN</td>
<td>YY</td>
<td>YY</td>
</tr>
<tr>
<td>Monaco</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Power Ledger</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Everex</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Decentraland</td>
<td>NN</td>
<td>YY</td>
<td>YY</td>
<td>YY</td>
</tr>
<tr>
<td>FunFair</td>
<td>YY</td>
<td>NN</td>
<td>YY</td>
<td>YY</td>
</tr>
<tr>
<td>Bitclave</td>
<td>YY</td>
<td>NN</td>
<td>YY</td>
<td>YY</td>
</tr>
<tr>
<td>Tierion</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>OmiseGo</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Aragon</td>
<td>NN</td>
<td>YY</td>
<td>YY</td>
<td>YY</td>
</tr>
<tr>
<td>0x</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Enjin</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>BlockV</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>FinShi Capital</td>
<td>Unauditable</td>
<td>Unauditable</td>
<td>Unauditable</td>
<td>ModificationNY</td>
</tr>
<tr>
<td>UTRUST</td>
<td>YY</td>
<td>NN</td>
<td>YY</td>
<td>YY</td>
</tr>
<tr>
<td>Target Coin</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>ATB Coin</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
<tr>
<td>Giga Watt</td>
<td>YY</td>
<td>NN</td>
<td>NN</td>
<td>NN</td>
</tr>
</tbody>
</table>

---

353 Storj is a hard case. It does have a token-based vesting regime, but not in the original smart contract, but rather in a subsequent one. See https://etherscan.io/address/0x34f34f58c50ef059b766065dbb24f7cf885e16463. We believe that the project team manually transferred tokens for lockup into that second contract. For our purposes, we do not count this as vesting being automatically accomplished through token design, though reasonable minds could disagree.

354 An early draft erroneously listed Enjin as YN.