8-2017

Blockchain's Treacherous Vocabulary: One More Challenge for Regulators

Angela Walch
St. Mary's University School of Law, awalch@stmarytx.edu

JOURNAL OF INTERNET LAW
VOLUME 21
NUMBER 2
AUGUST 2017
EDITED BY DLA PIPER

Blockchain's Treacherous Vocabulary: One More Challenge for Regulators

By Angela Walch

In February 2017, the Arizona state legislature passed a statute that was celebrated by the blockchain community as a sign that regulators were finally getting it.[1] The statute allows signatures "secured through a blockchain" to be treated as "electronic signatures"[2] and enables the use of blockchain-powered smart contracts in commerce.[3] Crucially, the statute defines "blockchain technology" as "distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless." It further provides that "[t]he data on the ledger is protected with cryptography, is *immutable* and auditable and *provides an uncensored truth*."[4]

What a mess. Instead of celebrating, we should be lamenting this legislation as woefully uninformed and creating more problems than it solves. Focusing merely on the statute's definition of "blockchain technology," numerous problems become evident. First, rather than being an inherent characteristic, "immutability" of blockchain records is a matter of debate,[5] as high-profile events in the blockchain space have shown that blockchain records are changeable at will by the people who comprise the blockchain system,[6] and it currently is unclear which variations of blockchain technology actually create a record that even approaches immutability.[7]

Simply stating in a statute that "data on the ledger is … immutable" does not *actually* make data immutable. This raises complicated questions. Do the legislators intend for data on a blockchain to be treated *as if* it is immutable, even if real-world events already have shown that it is not? (Think

Continued on page 10

Angela Walch *is an Associate Professor at St. Mary's University School of Law and a Research Fellow at the Centre for Blockchain Technologies at University College London. This essay is adapted from Angela Walch, "The Path of the Blockchain Lexicon (and the Law)," 36* Rev. Banking & Fin. L. *[ ] (2017) (forthcoming).*

Wolters Kluwer

Blockchain's Treacherous Vocabulary: from page 1

back to the July 2016 Ethereum hard fork when the blockchain record was rewritten to recover funds stolen from the hacked DAO.)[8] Or are they using the word "immutable" to mean something other than its normal meaning of "unchangeable," but just not being explicit about it? What if public and private blockchains actually differ in their ability to create "immutable" records (which is one position in the technology debate),[9] but the statute states that both types do?

Second, the statute states that "the data on the ledger … provides an uncensored truth."[10] Again, this is a vast overstatement of the technology's capabilities, as the truth of any data appearing on a blockchain ledger (other than perhaps the transfer of the native token itself) is limited by the quality or truth of the data entered on the ledger. If a false piece of data is put on a blockchain ledger, it remains false, regardless of the fact that it appears on the ledger (the garbage in/garbage out idea). The "uncensored truth" language in the statute echoes the lingo of the cypherpunk and crypto-anarchist groups that Bitcoin emerged from, and is bizarrely political and out-of-place in a statute. The language raises similar issues to the use of "immutable" in the statute, as it suggests that data on a blockchain ledger *is true* even if it isn't. Does that mean we should treat demonstrably false data as true, just because it appears in a blockchain record? How would that make sense?

Even this cursory analysis of the Arizona statute's definition of blockchain technology demonstrates that big problems can be created by legislating without an understanding of the relevant subject matter. Worryingly, the issues with the Arizona statute reflect a poor comprehension of blockchain technology and a failure to critically analyze the subject by the legislature and the governor who signed the statute into law. With regulators and policy makers around the world grappling with how to handle the much-hyped technology, the Arizona statute provides just one example of how things can go wrong, particularly when regulators do not carefully scrutinize the technological jargon they use. With numerous influential people touting blockchain technology as revolutionary for countless important social systems, from voting, to property records, to finance, it is critical for regulators and policy makers to get it right, even more so as government policy makers consider implementing the technology in their own consequential systems.

With Arizona's problematic statute as backdrop, this essay focuses on the fast-moving, contested, and often confusing language around blockchain technology, and the challenges this terminology muddle raises for regulators. After illuminating the language problems and their significance, I suggest ways that regulators can overcome the confusion and misunderstanding so easily generated by blockchain technology's unsettled vocabulary. In order for regulators, policy makers, and potential adopters to make the best decisions about blockchain technology, they must understand its *actual* characteristics, capabilities, and risks. Penetrating the language barriers around blockchain technology is essential to gaining this understanding, and therefore to responsibly and effectively use the technology. Moreover, actions such as those of the Arizona legislature demonstrate that there is no time to waste in the education process.

THE BLOCKCHAIN VOCABULARY VORTEX

As blockchain technology has gained attention from the financial sector and others, its vocabulary has rapidly grown and changed. Copious jargon is used in the field, often imprecisely. Many different terms are somewhat overlapping, increasing the confusion. For example, "blockchain technology" also is referred to as "distributed ledger technology" or "DLT" or "shared ledger technology" or "SLT" or a "distributed database." There is an emerging sense that blockchain technology is a subcategory of DLT, but that is not yet resolved. Other examples of terminology problems include inconsistency in referring to the record generated by blockchain technology as "tamper-proof" versus "tamper-evident" or "tamper-resistant." Each of these presumably means something very different about the reliability or robustness of the blockchain record, yet the terms often seem to be used indiscriminately. Numerous other examples of contested terms abound (*e.g.*, immutable, trustless, decentralized), as I explore more deeply in a lengthier forthcoming article,[11] and awareness of the terminology problems within the blockchain ecosystem is growing, as evidenced by numerous articles seeking

to provide definitions of contested terms,[12] and efforts by international organizations to begin to standardize the terminology.[13]

Language in general is always on the move, but is particularly fluid around a fast-moving innovation such as blockchain technology. As the technology is tweaked, new terms are created to distinguish the new version from the old, as has occurred with the creation of the terms "permissionless" and "permissioned" blockchains to distinguish the original open blockchains such as Bitcoin from new ones that have a limited and known set of transaction processors in the network. Further, new terms are introduced as the original ones are rethought, perhaps as understanding of the technology's capabilities shifts. For example, a blockchain record generally has been described as "tamper-proof," an extremely bold claim suggesting it is impossible to alter; it is becoming more common, however, to see it described as "tamper-evident" or "tamper-resistant," which are more modest claims about the record's strength.

Blockchain technology's terminology also has shifted for marketing, or commercial purposes. For instance, when Bitcoin became associated with the criminal underworld of money laundering and the illegal goods marketplace Silk Road, people began talking about the potential offered by "blockchain technology" rather than Bitcoin itself, and a number of companies with "Bit" in their names changed them to escape the Bitcoin taint.[14] Finally, the interdisciplinary nature of blockchain technology has contributed to vocabulary problems, as numerous fields (*e.g.*, cryptography, computer science, economics, etc.) have brought their own jargon to the discussion, making communication more confused.

REGULATORY CHALLENGES

Despite nascent standardization efforts, the difficulties with language remain, and are highly problematic for regulators and others seeking to learn about blockchain technology. Language barriers make it difficult for regulators to pin down the facts about the technology and to distinguish between different variations of the technology. Further, the confused language around the technology increases the potential for regulatory capture, as well as the potential for inconsistent regulation across jurisdictions. All of these challenges make it more likely for regulators to make flawed decisions about the technology, undermining their effectiveness in protecting consumers and in maintaining financial and social stability. Below, I discuss each of these challenges in turn.

First, the inconsistent, confusing, and sometimes misleading vocabulary around blockchain technology can make it difficult for regulators to get a handle on the "facts" about the technology.[15] For example, how robust is the record created by the technology? Is it *impossible* to change or tamper with, or just *really hard but possible*? Is the need to trust other people in a blockchain network actually *eliminated* through the use of the technology (making it "trustless"), or is trust just displaced to other parties? Does the use of blockchain technology to create a record make the data on the record more likely to be true, or does the reliability of the record ultimately depend on the quality of the data entered? Arriving at accurate answers to these questions is critical in understanding the technology's true capabilities and risk profile. It should go without saying that the better the regulator understands the subject matter, the better decisions he or she can make, whether in deciding the details and scope of regulation, or in deciding not to regulate at all.

Second, the muddled language around blockchain technology makes it difficult to distinguish between variations of the technology, complicating regulators' risk assessment process. Multiple variations of blockchain technology now exist, with each having different capabilities and risks. It is common, however, for all variations to be referred to as "blockchain technology," and to describe the entire diverse mix as having the same fundamental characteristics of immutability, security, and trustlessness. This makes it hard for regulators to grasp the true risk profile of a given form of blockchain technology, which means that their decisions related to the technology may be ill-informed. For example, should blockchains that use different consensus mechanisms to agree on the state of the blockchain record be treated the same or differently from a regulatory perspective? What about public versus private blockchains? A confused terminology makes these types of question more difficult to answer.

Third, the language haze can contribute to other problems for regulators, including increasing the chance of regulatory capture and all of the negative

effects that brings. "[R]egulatory capture occurs when bureaucrats, regulators and politicians cease to serve some notion of a wider collective public interest and begin to systematically favor specific vested interests, usually the very interests they were supposed to regulate and restrain for the wider public interest."[16] Regulatory capture is made more likely for blockchain technology because the confused vocabulary can increase regulators' dependence on blockchain industry experts to explain the technology to them. Of course, consulting with industry experts is essential to understand the facts well enough to make good regulatory decisions.

However, with blockchain technology, the terminology problems can make it easier for proponents of the technology to overstate the capabilities and benefits of the technology, while understating the risks and potential downsides. This is compounded by the complex, interdisciplinary nature of blockchain technology, which may make regulators less likely to interrogate industry's claims about the technology, as they may feel out of their depth. Worryingly, blockchain technology's opaque complexity mirrors that of the complicated financial products and risk models that contributed to the Financial Crisis. As regulators were "daunted by the complexity posed by the new financial instruments and awed by the promise of new financial engineering to shift and spread risk efficiently,"[17] they failed to understand the true risk profile of these financial creations. There is potential for similar deference by regulators towards blockchain technology.

Moreover, the potential for regulatory capture is further increased with blockchain technology because of the high number of prominent former regulators and well-respected businesspeople who are working for blockchain technology companies or serving as advisors or board members to them.[18] This means that regulators may have personal relationships with the people who are explaining the technology to them, or may be influenced by the reputation or prestige of the person associated with the technology. The strong possibility for "cognitive capture" or "cultural capture" of regulators by the blockchain technology industry increases the likelihood that misunderstandings about the technology (willfully or innocently introduced) will shape regulatory and policy decisions about it.[19]

Fourth, the unclear vocabulary around blockchain technology could lead to inconsistent regulation across jurisdictions. Striking differences in regulation could emerge across jurisdictions due to differing understandings of the capabilities and risks of the technology, even if regulators have aligning policy objectives. For instance, if one jurisdiction (such as Arizona) understands that a record created through blockchain technology (of whatever variation) is "immutable" and inevitably reflects "truth," then that jurisdiction may choose to give a blockchain record privileged status for evidentiary purposes. A jurisdiction that understands a blockchain record to be difficult but not impossible to alter, and the "truth" of the information stored on the record to be limited by the quality or truth of the information put into the record, may treat blockchain records the same as any other record under evidentiary rules. Both jurisdictions may have the same policy goal of structuring their rules of evidence to permit reliable information to be introduced in a case, but could wind up with wildly divergent treatment of the records, and potentially differing outcomes for a single set of facts.

Analogous inconsistencies in regulation could arise in other regulatory domains, including in setting reporting or disclosure obligations, standards for fraud, or multiple other possibilities. Inconsistent regulation can lead to forum shopping and regulatory arbitrage, as parties search for the most attractive legal regime. Further, diverging regulation can increase compliance costs for parties operating across multiple jurisdictions, as is likely for blockchain technology with its effortless spanning of borders.

As this brief discussion makes clear, the vocabulary problems around blockchain technology can generate serious consequences, making it crucial for regulators and others seeking to understand the technology to be acutely alert to the presence of language issues, and to utilize the critical approach to the technology that I recommend below.

PENETRATING THE LANGUAGE BARRIER

What can regulators and others seeking to understand blockchain technology do to fight through the language barrier surrounding it? Simply being aware that blockchain vocabulary is treacherous can help, as can a critical approach to the learning process. Presumably this is the approach everyone already takes when learning about a new topic, but sometimes

a reminder of these basic principles is worthwhile. As the Financial Crisis made clear, we often either assume we understand something well, or pretend to understand something well, when the reality is that we have failed to perceive critical facts and implications of a given subject. In this section, therefore, I highlight the mindset and learning strategies that can help regulators and others achieve a more accurate and nuanced understanding of blockchain technology's risks and benefits.

INTERROGATE HYPE

Hype about blockchain technology is rampant, with many making grand claims about its ability to solve vexing human problems such as financial inclusion, corrupt governments, delays to settlement of transactions, and many more. Unfortunately, blockchain's language problems can make it more difficult to distinguish hype from reality. For instance, it is common to see references to "the blockchain" or just "blockchain" when people describe the benefits of the technology, which is problematic given the vast differences in features among different forms of the technology. Grouping all variations of the technology under the label "blockchain" can lead to major misunderstandings about each variant's risks and capabilities, and regulators must be alert to this potential as they work to grasp the truth about the technology.

BE SKEPTICAL OF EVERYONE AND EVERY FORUM

"Fake news" is everywhere in the blockchain technology space, and can even show up in reputable sources, often cloaked in terminology problems. For example, a number of sources in reputable fora have stated that Estonia used blockchain technology in its national digital identity system,[20] but Estonian officials and historic records indicate this is untrue.[21] Further, I and others have questioned the appropriateness of the term "immutable" to describe a record created by blockchain technology;[22] the term is omnipresent in blockchain discourse, including in reports and articles in prestigious publications, making misunderstanding about the technology's capabilities likely.[23] These types of inaccurate or misleading statements, whose inaccuracy can be masked by problematic vocabulary, can become embedded in the discourse, as an inaccuracy is cited as true again and again.

This means that one cannot assume that a given forum, whether publication or venue, will provide accurate information about blockchain technology. Misleading or inaccurate statements and language about the technology appear in sources that are treated as authoritative and reliable by default, often because of the source's history or an association with a prestigious and trusted institution.[24] So, skepticism about claims made regarding blockchain technology is warranted, regardless of the legitimacy or prestige of the forum where the claim is made. Regulators must recognize that traditional markers of legitimacy are insufficient to assume reliable information about blockchain technology, and should therefore thoroughly probe every claim.

IDENTIFY AND WEIGH CONFLICTS OF INTEREST

As with any new industry, there is a lot of money up for grabs in the blockchain technology space, and regulators must keep in mind that people's financial incentives can influence their view of the technology, its potential, and its risks. Much of the education of regulators and policy makers is being performed by blockchain industry lobbying organizations, such as the Digital Chamber of Commerce, the Global Blockchain Business Council, and the industry-funded think tank and advocacy organization Coin Center. This does not mean that the information provided by such organizations necessarily is misleading or wrong, but regulators must be alert to how industry incentives can impact their input, and weigh how these conflicts affect the reliability of the information and recommendations of these groups.

"Everybody's got an angle"[25] in the blockchain space, from industry players to the numerous and vocal thought leaders, and regulators must sniff out each party's angle and weight its perspective accordingly.

SEEK DIVERSE POINTS OF VIEW

In the last few years, a consensus has rapidly formed that blockchain technology is a revolutionary

innovation that will transform a wide swath of industries and practices. As the consensus has spread, few dissenting opinions have been expressed. This quick agreement means it is likely that there are many critical questions about the technology, its capabilities, and its risks that have not been answered or even asked.

Regulators should therefore seek out diverse perspectives in learning about blockchain technology to help them to avoid misunderstandings and group think. This means that they should solicit input from critics of the technology as well as proponents; from those who see the benefits and risks of blockchain technology as great as well as those who see them as small or somewhere in the middle. They should seek advice from people from different academic disciplines and business areas, given the extreme interdisciplinarity of blockchain technology. Similarly, other forms of diversity, including gender, race, economic, and geographic diversity, can help regulators gain a more nuanced, complete understanding of the technology. The benefits of a diverse group of decision-makers are well known,[26] and regulators must ensure that their learnings are as fulsome as possible.

DON'T SKIP ANALYTICAL STEPS (DON'T ASSUME FOUNDATIONS ARE SOLID)

As mentioned previously, one reason the vocabulary around blockchain technology is so unsettled is that the technology is evolving so rapidly. Nothing is settled about blockchain technology, including *what it is*, its features, or its flaws. These are the subject of much experimentation and debate amongst technologists and entrepreneurs in the space. Yet policy makers and regulators often jump ahead to questions of the implications of the technology—how can we use it to solve problems, or prevent it from being used improperly—and assume that foundational facts about the technology are settled.

Because both the technology and its vocabulary are so fluid and immature, regulators must ask questions about *everything*. Does the technology *actually* create immutable records in a secure or trustless way? How, *precisely*, does it do this? How does each variation to the technology, whether in the consensus mechanism, the permitted validators, or the cryptography selected, alter the capabilities and risks of the technology? What assumptions are technologists and businesses making that are left unsaid? What does every word of jargon mean to the person who uses it?

Any less-thorough inquiry is inadequate, given the combination of language issues, complexity, and hype that surround this fast-moving technology.

DON'T BE A LEMMING

Regulators and policy makers face significant pressures to act in particular ways. They often are caught in the uncomfortable position of being blamed for not being innovative enough and killing jobs with inappropriate regulation, while at the same time, they are criticized if they inadequately protect consumers or fail to prevent or adequately manage a crisis (with the Financial Crisis likely a searing memory for many).

This can make it tempting to just do what other regulators and policy makers are doing, so that one can't be individually blamed down the road for making a bad decision. There are benefits to conformity, one of which is diffusion of accountability. Herd behavior, "the phenomenon [in which]…everyone does what everyone else is doing, even when their private information suggests doing something quite different,"[27] can manifest among regulators[28] as well as in the adoption of new technologies.[29] No one wants to be seen as restricting innovation or to miss out on a useful new technology, so when regulators see others contemplating introducing a central bank digital currency, or using blockchain technology for government processes, they may feel compelled to join in.

Regulators and policy makers need to be willing to swim against the current until they have investigated blockchain technology thoroughly and have developed their own, well-founded knowledge about it. Only then they can make useful regulatory choices (including decisions not to regulate at all) or decide whether adoption of the technology is appropriate.

CONCLUDING THOUGHTS

Flawed understandings of blockchain technology can yield poor regulation and inappropriate adoption of the technology in critically important systems. It is crucial that regulators and policy makers actually

understand what they are grappling with before making regulatory decisions (including whether to regulate at all). The rapidly-changing, contested, and often misleading vocabulary around blockchain technology makes regulators' task that much more difficult, as the facts end up buried beneath a muddle of impenetrable gibberish.

Rather than throwing up their hands, regulators, policymakers, and those considering adopting the technology must take a critical, deliberative approach to learning about blockchain technology, with awareness that language issues can obscure reality and lead to misunderstandings. With critically important social systems being vetted for the technology's use, and regulators and policy makers taking actions as we speak, this matter is incredibly urgent, and must be brought immediately to the attention of blockchain decision-makers. I close then, dear reader, with a request: don't just sit on this information—go out and spread the word!

NOTES

1. *See* Jeffrey D. Neuberger, "Arizona Passes Groundbreaking Blockchain and Smart Contract Law—State Blockchain Laws on the Rise," *The Nat. L. Rev.* (April 20, 2017), *https://www.natlawreview.com/article/arizona-passes-groundbreaking-blockchain-and-smart-contract-law-state-blockchain* (reporting on Arizona's blockchain statute and other state legislatures' activities around blockchain technology).
2. Act of Sept. 21, 2006, ch. 26, Ariz. Rev. Stat. Ann. § 44-7003 (2006) (amended by 2017 Ariz. Sess. Laws 2417), *https://legiscan.com/AZ/text/HB2417/id/1528949*.
3. *Id.*
4. H.B. 2417, 53rd Leg., 1st Reg. Sess. (Ariz. 2017) (emphasis added).
5. *See* Angela Walch, "The Path of the Blockchain Lexicon (and the Law)," 36 *Rev. Banking & Fin. L.* [ ] (2017) (forthcoming) (exploring the misleading use of the term "immutable" in describing blockchain technology); Gideon Greenspan, "The Blockchain Immutability Myth," *CoinDesk* (May 9, 2017), *http://www.coindesk.com/blockchain-immutability-myth/* ("In blockchains, there is no such thing as perfect immutability.").
6. *See* Walch, *supra* n.5, at Part IV (describing how previous forks in public blockchains such as Bitcoin and Ethereum demonstrate that blockchain records are not immutable).
7. *See id.* (discussing the debate over what combination of features in the wide spectrum of blockchain technology variations gives rise to "immutable" records).
8. *See* Kevin D. Werbach, "Trustless Trust," 66-68, (Aug. 14, 2016) (unpublished manuscript), *https://ssrn.com/abstract=2844409* (providing a succinct overview of the events surrounding the July 2016 Ethereum hard fork).
9. Nitesh Emmadi & Harika Narumanchi, "Reinforcing Immutability of Permissioned Blockchains with Keyless Signatures' Infrastructure," in International Conference on Distributed Computing and Networking (2017) 1-2 (describing how immutability of the ledger cannot be guaranteed in permissioned blockchains and proposing remedies to guarantee immutability in permissioned settings).
10. H.B. 2417, 53rd Leg., 1st Reg. Sess. (Ariz. 2017).
11. *See* Walch, *supra* n.5 (exploring the misleading use of the term "immutable" in describing blockchain technology).
12. *See, e.g.*, Sebastien Meunier, "Blockchain Technology—a Very Special Kind of Distributed Database" (Dec. 29, 2016), *https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118#.oywrg7q0r* (providing a taxonomy of distributed database technology); Colin Platt, "Thoughts on the Taxonomy of Blockchains & Distributed Ledger Technologies," *Medium* (Feb. 27, 2017), *https://medium.com/@colin_/thoughts-on-the-taxonomy-of-blockchains-distributed-ledger-technologies-ecad1c819e28#.6gktvnu8k* (proposing a taxonomy for the variations of blockchain technology).
13. *See, e.g.*, Clare Naden, "Blockchain technology set to grow further with international standards in pipeline," *Int'l Org. for Standardization*, (May 24, 2017), *https://www.iso.org/news/Ref2188.htm* (reporting on work on ISO TC 307 related to blockchain technology).
14. *See* Tim Swanson, "The great pivot? Or just this years froth?," *Great Wall of Numbers* (Oct. 16, 2015), *http://www.ofnumbers.com/2015/10/16/the-great-pivot-or-just-this-years-froth/*; Stan Higgins, "ItBit Rebrands as Paxos Amid Blockchain Pivot," *CoinDesk* (Sept. 14, 2016), *http://www.coindesk.com/itbit-rebrands-paxos-amid-blockchain-pivot/*; Pete Rizzo, Adam Draper; "Investors Don't Want to Hear the Word Bitcoin," *CoinDesk* (Oct. 19, 2015), *http://www.coindesk.com/adam-draper-investors-bitcoin-blockchain/* (discussing the "vernacular change" from "Bitcoin" to "blockchain" in investor interest).
15. *See* Mark Fenwick et al., "Regulation Tomorrow: What Happens When Technology is Faster than the Law?," Tilburg Univ., TILEC Discussion Paper No. 2016-024, 2016, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2834531* (providing an overview of how innovative practices and technologies create regulatory challenges and discussing the need for regulators to decide relevant facts before making regulatory decisions).
16. *See* Andrew Baker, "Restraining Regulatory Capture? Anglo-America, Crisis Politics and Trajectories of Change in Global Financial Governance," 86 *International Affairs*, No. 3, 2010, at 648.
17. Erik Gerding, "Code, Crash, and Open Source: The Outsourcing of Financial Regulation to Risk Models and the Global Financial Crisis," 84 *Wash. L. Rev.* 127, 134 (2009) (describing how regulators accepted that the financial sectors' complex risk models and financial products could adequately manage risk, and how problems with the models contributed to the Financial Crisis).
18. Along with many other former regulators, policy makers, and influencers, former US Treasury Secretary Lawrence A. Summers, former SEC Chairman Arthur Levitt, former CFTC Commissioner Mark Wetjen, former New York Superintendent of Financial Services Ben Lawsky, and former Chair of the FDIC Sheila Bair have associated themselves with Bitcoin or the blockchain technology space. *See* Walch, *supra* n.5 at Part III.
19. Arthur E. Wilmarth, Jr., "Turning a Blind Eye: Why Washington Keeps Giving In to Wall Street," 81 *U. Cin. L. Rev.* 1283, 1417-1418 (2013) (citations omitted) ("[E]xtensive professional and social contacts encourage regulators to align themselves with the outlook of industry officials, a phenomenon that analysts have described as "cultural capture" and "cognitive capture."…The likelihood of cultural capture increases when (i) financial regulators feel part of an "in-group" with industry executives due to close professional contacts and shared "social networks," and (ii) regulators view industry insiders as occupying a "higher status" based on wealth, intellectual achievement and social prominence.").
20. *See, e.g.*, Dave Birch, "House of Blockchain," *Consult Hyperion* (Dec. 7, 2016), *http://www.chyp.com/house-of-blockchain/* (stating

that discussion of blockchain technology in United Kingdom's House of Lords included incorrect statements that the Estonian digital identity system used blockchain technology); Michael Mainelli, "Blockchain Will Help Us Prove Our Identities in a Digital World," *Harv. Bus. Rev.* (Mar. 16, 2017), *https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world* (stating that "since 2007 Estonia has been operating a universal national digital identity scheme using blockchain); Don Tapscott, "New Economy Talks with Don Tapscott," *Int'l Monetary Fund* (Oct. 6, 2016), *http://www.imf.org/external/mmedia/view.aspx?vid=5160059156001* (quoting Don Tapscott at the 42 minute mark, "Estonia showing the way forward with the blockchain-based identity").

21. *See* Dave Birch, Estonia, "Fake news and digital identity," *Consult Hyperion* (Mar. 20, 2017), *http://www.chyp.com/estonia-fake-news-and-digital-identity/* (debunking the "urban legend" that Estonia's digital identity system uses a blockchain).
22. *See* Walch, *supra* n.5, Part IV (arguing that the use of the term "immutable" to describe the records created by blockchain technology is inappropriate and misleading); Greenspan, *supra* n.5 ("In blockchains, there is no such thing as perfect immutability.").
23. *See, e.g.*, Andrea Tinianow & Caitlin Long, "Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance," *Harv. L. Sch. F. on Corp. Governance & Fin. Reg.* (Mar. 16, 2017), *https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/* ("Distributed ledgers … create a single record of transactions among multiple parties, providing one immutable, "golden copy" of data that all parties *see* at the same time and can trust as valid."); Marc Pilkington, Blockchain Technology: Principles & Applications, in Research Handbook on Digital Transformations 15 (F. Xavier Olleros & Majlinda Zhegu eds., 2016) ("Immutability is a characteristic of blockchain technology."); Chamber of Dig. Commerce & Ctr. for Fin. Mkts. & Policy at Georgetown Univ. McDonough Sch. of Bus., Blockchain and Financial Inclusion 8 (2017), *http://finpolicy.georgetown.edu/sites/finpolicy.georgetown.edu/files/Blockchain%20and%20Financial%20Inclusion%20120417.pdf* ("The disruptive component of blockchain technology is that its core functionality depends on the creation of an immutable ledger …") (emphasis added to all quotations).
24. *See, e.g.*, sources found in *supra* ns.20, 23.
25. As stated by Bing Crosby's character in 1954s White Christmas.
26. *See generally* Scott E. Page, The Difference (2008) (exploring how different types of diversity improve problem solving in groups).
27. Heshan Sun, "A Longitudinal Study of Herd Behavior in the Adoption and Continued Use of Technology," 37 *Mgmt. Info. Sys. Q.* 1013, 1014 (2013) (citations omitted).
28. *See* Tom C.W. Lin, "The New Financial Industry," 65 *Ala. L. Rev.* 567, 608 (2014) ("Too much coordination [among regulators] could lead to "destructive coordination," which could result in thoughtless herd behavior by regulators and participants. Too much coordination can also erode competition among regulators with different areas of focus and expertise.") (citations omitted).
29. *See* Sun, *supra* n.27, at 1014 (stating that herd behavior "may explain why people quickly converge on the same form of technology by imitating each other's choices. … [W]hen herding, people may later reexamine and reverse their initial decisions, somewhat accounting for the en masse abandonment of a particular technology").