

# Insider Trading and Cryptoassets: The Waters Just Got Muddier

*John P. Anderson\**

I.	INTRODUCTION.....	120
II.	EXISTING PROBLEM OF VAGUENESS IN LAW OF INSIDER TRADING.....	121
III.	FURTHER AMBIGUITY IN CONTEXT OF CRYPTOASSETS .....	123
IV.	CONCLUSION .....	129

## I. INTRODUCTION

Imagine the following scenario. In January of 2019, a group of tech developers make an initial coin offering (ICO) to raise capital for their new cryptocurrency, Geekcoin. In advance of the ICO, Geekcoin is promoted as introducing superior blockchain technology. Two months after its successful launch, Geekcoin steadily gains in price and volume, and begins to build a reputation as an up-and-coming cryptocurrency. By March of 2019, however, Geekcoin was still not being traded on one of the most prominent digital currency exchanges, Cryptobase. On March 15 of 2019, Cryptobase management called a meeting of its employees and the CEO announced that the exchange will begin supporting Geekcoin transactions on April 1, and that the employees were to keep this information confidential until that time. One employee raised her hand and asked, “Are we permitted to trade in Geekcoins ourselves prior to that date?” The CEO responded, “Yes, our employees may trade in Geekcoins prior to the announcement, but you may not share the news with nonemployees.”

Cryptobase employees immediately started buying Geekcoins on other exchanges in anticipation of the April 1 announcement, and the price of Geekcoins jumped from \$1 per coin on March 15 to \$5 per coin on March 31. The price of Geekcoins jumped to \$10 when the announcement was made on April 1.

When word got out that Cryptobase employees were trading in advance of the April 1 announcement, many traders who had sold their Geekcoins

---

\* Professor, Mississippi College School of Law.

between March 15 and March 31 were outraged. Seeing this as an opportunity to make a name for himself in the emerging world of crypto-crime, an enterprising prosecutor opens an insider trading investigation of Coinbase, its CEO, and all of the employees who traded in Geekcoins in advance of the announcement.

Though this scenario is fictitious,<sup>1</sup> it is not far-fetched—and, for reasons offered below, this is troubling.

## II. EXISTING PROBLEM OF VAGUENESS IN LAW OF INSIDER TRADING

In October 2018, former U.S. Attorney Preet Bharara and SEC Commissioner Robert J. Jackson co-authored a *New York Times* op-ed in which they lamented the “shoddy state of American insider-trading law.”<sup>2</sup> According to Bharara and Jackson, the principal problem for the current regime is its lack of a clear statutory definition.<sup>3</sup>

Section 10(b) of the Exchange Act provides the principal statutory authority for insider trading enforcement, but it makes no reference to insider trading.<sup>4</sup> Section 10(b) offers a general anti-fraud provision, prohibiting the employment of “any manipulative or deceptive device or contrivance” used, “in connection with the purchase or sale of any security.”<sup>5</sup>

Though Section 10(b) was designed as a “catchall,” the Supreme Court has made it clear “what it catches must be fraud.”<sup>6</sup> But while fraud typically requires an affirmative misrepresentation, insider trading usually involves silence or a failure to disclose while trading over an anonymous exchange.<sup>7</sup> Recognizing that the common law only deems silence to be fraudulently deceptive where circumstances impose a duty to disclose, the Supreme Court has consistently held that insider trading liability requires proof of some breach of a fiduciary (or similar) duty of trust and confidence.<sup>8</sup> The Court has recognized two theories whereby a duty to disclose is owed.

Under the classical theory, insider trading liability arises where the issuer, its employee, or someone otherwise affiliated with the issuer seeks to benefit from trading (or tipping others who trade) that firm’s shares based on material nonpublic information.<sup>9</sup> In such cases, the insider (or constructive

1. Though fictitious, the scenario is loosely based on the facts alleged by the civil complaint in *Berk v. Coinbase, Inc.* See Class Action Complaint at 1–3, *Berk v. Coinbase, Inc.*, No. 4:18-cv-01364-KAW (N.D. Cal. March 1, 2018).

2. Preet Bharara & Robert J. Jackson Jr., *Insider Trading Laws Haven’t Kept Up with the Crooks*, N.Y. TIMES (Oct. 9, 2018), <https://www.nytimes.com/2018/10/09/opinion/sec-insider-trading-united-states.html> [<https://perma.cc/FX36-7WCL>].

3. *Id.*

4. 15 U.S.C. § 78j(b) (2018).

5. *Id.*

6. *Chiarella v. United States*, 445 U.S. 222, 234–35 (1980).

7. See, e.g., *id.* at 227–28; *Dirks v. S.E.C.*, 463 U.S. 646, 654–55 (1983); *United States v. O’Hagan*, 521 U.S. 642, 651–52 (1997); *Salman v. United States*, 137 S. Ct. 420, 423 (2016).

8. See, e.g., *Chiarella*, 445 U.S. at 227–29.

9. See, e.g., *O’Hagan*, 521 U.S. at 651–52.

insider) violates a fiduciary (or similar) duty of trust and confidence by failing to disclose to the firm's shareholder(s) (or prospective shareholder(s)) on the other side of the trade.<sup>10</sup>

Under the misappropriation theory, insider trading liability arises where one misappropriates material nonpublic information and then seeks to benefit by trading on it (or by tipping others who trade on it) without first disclosing the intent to trade to the source of the information.<sup>11</sup> The "misappropriation theory premises liability on a fiduciary-turned-trader's deception of those who entrusted [her] with access to confidential information" by cheating them out "of the exclusive use of that information."<sup>12</sup>

The mere fact that insider trading law in the U.S. is essentially judge made is a "scandal" in itself.<sup>13</sup> As Professor Miriam Baer and others have noted, such common-law crimes risk violating the Western liberal jurisprudential principal of legality,<sup>14</sup> which demands that "there must be no crime or punishment except in accordance with fixed, reasonably specific, and fairly ascertainable preestablished law."<sup>15</sup> This principle is rarely satisfied when criminal liability is expanded by judicial precedent, as it was, for example, when the misappropriation theory of insider trading liability was first recognized by the Supreme Court in 1997.<sup>16</sup> But matters are made worse by the fact that even the well-established common-law elements of insider trading are exceedingly vague and ill-defined.

For example, courts and regulators have struggled (and failed) to reach consensus on when information is "based upon" material nonpublic information, when information is "material," when it is "nonpublic," what constitutes a "fiduciary or similar relation of trust and confidence," what constitutes a "benefit" in the context of tipper/tippee liability, and there is even disagreement among the courts over what mental state is required to satisfy each of these elements.<sup>17</sup>

According to Bharara and Jackson, this lack of statutory definition and vagueness in the common-law elements of insider trading liability has resulted in "a legal haziness that leaves both investors and defendants unclear about what sorts of information-sharing or other activities by investors would be

---

10. See *Chiarella*, 445 U.S. at 228.

11. See, e.g., *O'Hagan*, 521 U.S. at 652.

12. *Id.*

13. Jeanne L. Schroeder, *Taking Stock: Insider and Outsider Trading by Congress*, 5 WM. & MARY BUS. L. REV. 159, 163 (2014) ("[T]he jurisprudential scandal that insider trading is largely a federal common law offense.").

14. See generally Miriam H. Baer, *Insider Trading's Legality Problem*, 127 YALE L.J.F. 129 (2017) (detailing the problems with handling insider trading as a common-law crime as opposed to a statutory crime); see also John P. Anderson, *Anticipating a Sea Change for Insider Trading Law: From Trading Plan Crisis to Rational Reform*, 2015 UTAH L. REV. 339, 369-71 (2015).

15. DAVID A.J. RICHARDS, *THE MORAL CRITICISM OF LAW* 195 (1977).

16. See *O'Hagan*, 521 U.S. at 652.

17. See, e.g., JOHN P. ANDERSON, *INSIDER TRADING: LAW, ETHICS, AND REFORM* 59-87 (2018).

considered insider trading.<sup>18</sup> Indeed, the problem of vagueness in the law of insider trading has come to be viewed (by prosecutors, regulators, and the defense bar alike) as so bad that Bharara and Jackson announced the creation of the Bharara Task Force on Insider Trading to propose reforms.<sup>19</sup>

In the midst of such legal uncertainty, the fact that regulators are beginning to “eye cryptocurrency and cryptocurrency derivative products for insider trading abuses” promises to further muddy the waters.<sup>20</sup>

### III. FURTHER AMBIGUITY IN CONTEXT OF CRYPTOASSETS

In *SEC v. W.J. Howey Corp.*, the Supreme Court offered a four-prong test for determining whether an investment contract qualifies as a “security” under Section 2(a)(1) of the Securities Act of 1933 and Section 3(a)(10) of the Securities Exchange Act of 1934.<sup>21</sup> Under *Howey*, “[t]he test is whether the scheme involves [1] an investment of money [2] in a common enterprise [3] with profits to come [4] solely from the efforts of others.”<sup>22</sup> Controversy has arisen over the application of all four of these prongs to cryptoassets, but most of the debate focuses on the third and fourth prongs.<sup>23</sup>

For example, most ICOs are launched by promoters who “tout their ability to create an innovative application of blockchain technology.”<sup>24</sup> And, as William Hinman, SEC Director, Division of Corporation Finance, recently explained, at this early stage of a network’s development, “the business model and very viability of the application is still uncertain.”<sup>25</sup> The purchaser therefore “usually has no choice but to rely on the efforts of the promoter to build the network and make the enterprise a success.”<sup>26</sup> Under such circumstances, the purchase of coins or tokens offered through an ICO would

---

18. Bharara & Jackson, *supra* note 2.

19. *Id.*

20. Jason P. Gottlieb, Daniel C. Isaacs & Christopher W. Pendleton, *Insider Trading and Cryptocurrency: A Primer for Traders*, BLOOMBERG L. (Feb. 15, 2018, 4:58 PM), <https://news.bloomberglaw.com/tech-and-telecom-law/insider-trading-and-cryptocurrency-a-primer-for-traders> [<https://perma.cc/8GUG-MKMN>].

21. Sec. Exch. Comm’n v. W.J. Howey Corp., 328 U.S. 293, 297–301 (1946); *see* 15 U.S.C. § 77b(a)(1) (2018); 15 U.S.C. § 78c(a)(10). Although definitions in these provisions are slightly different, “the two definitions have been held to be ‘virtually identical.’” Sec. Exch. Comm’n v. Blockvest, LLC, No. 18CV2287-GPB(BLM), 2018 WL 6181408, at \*5 (S.D. Cal. 2018) (citing *Amfac Mort. Corp. v. Ariz. Mall of Tempe, Inc.*, 583 F.2d 426, 431 (9th Cir. 1978)).

22. *Howey*, 328 U.S. at 301.

23. *See, e.g.*, STRATEGIC HUB FOR INNOVATION & FIN. TECH., SEC, FRAMEWORK FOR ‘INVESTMENT CONTRACT’ ANALYSIS OF DIGITAL ASSETS 2–8 (Apr. 4, 2019), <https://www.sec.gov/files/dlt-framework.pdf> [<https://perma.cc/2VAS-2MMJ>] [hereinafter APRIL 2019 GUIDANCE STATEMENT] (noting that the “investment of money” prong is “typically satisfied” in an ICO, and that the SEC has found that a “common enterprise . . . typically exists” as well).

24. William Hinman, Dir., Div. of Corp. Fin., Remarks at the Yahoo Finance All Markets Summit: Crypto, (June 14, 2018), <https://www.sec.gov/news/speech/speech-hinman-061418#XBqZoWITv9U.email> [<https://perma.cc/gMM5-HGKJ>] [hereinafter Hinman, *Remarks*].

25. *Id.*

26. *Id.*

likely satisfy the third and fourth prong of the *Howey* test.<sup>27</sup> Initial investors are purchasing coins or tokens with the expectation of profits from a successful launch.<sup>28</sup> Director Hinman’s application of the *Howey* test to tokens or coins issued through ICOs and traded shortly thereafter is fairly intuitive, though not entirely without controversy.<sup>29</sup>

But serious problems arise when one considers the fact that, while the distributed ledger technology supporting a given digital asset may be initially developed and marketed by an identifiable individual or group, once launched, the network’s ultimate success will depend on its *decentralization*.<sup>30</sup> Hence, at the outset, both purchasers and promoters should expect that, soon after the launch, the network will be so decentralized that it will no longer depend on the entrepreneurial or managerial skills of the promoters for its operation or success. Once this hope is realized, however, the fourth prong of *Howey* is no longer satisfied. Recognizing this, the SEC seems prepared at this stage to no longer regard coins or tokens supported by such a network as securities.<sup>31</sup>

So, for example, the 72 million “pre-mined” Ether coins that were issued in the July/August 2014 crowdsale to capitalize the Ethereum network and its development team<sup>32</sup> may have been securities, with purchasers relying on the entrepreneurial and managerial talents of Vitalik Buterin and his team to design and implement a secure and successful network that would increase

27. *Id.*

28. *Id.* (“Funds are raised with the expectation that the promoters will build their system and investors can earn a return on the instrument—usually by selling their tokens in the secondary market once the promoters create something of value with the proceeds and the value of the digital enterprise increases.”).

29. *See, e.g.*, Sec. Exch. Comm’n v. Blockvest, LLC, No. 18CV2287-GPB(BLM), 2018 WL 6181408, at \*5 (S.D. Cal. 2018) (holding that the SEC failed to show tokens offered to test investors ahead of a planned ICO were securities). *See also* the controversy over “pre-mined” (or “minted”) and openly mined tokens below. *See infra* notes 31–45 and accompanying text.

30. For example, Bitcoin’s white paper, authored by the pseudonymous Satoshi Nakamoto, explains:

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double spending.

Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG, <https://bitcoin.org/bitcoin.pdf> [<https://perma.cc/64WW-WU7G>] (last visited Aug. 23, 2020). The key to the cryptocurrency’s success is that “[t]here is no central authority who controls the ledger or who can censor specific transactions.” ANTONY LEWIS, *THE BASICS OF BITCOINS AND BLOCKCHAINS* 193 (2018). The same is true of Ethereum: “The vision of Ethereum is to create an unstoppable, censorship resistant, self-sustaining, decentralized, world computer.” *Id.* at 254.

31. *See* Hinman, *Remarks, supra* note 24. Indeed, some digital assets may be decentralized from the outset. For example, Director Hinman notes that it is likely that Bitcoin may have been decentralized from its inception and therefore never relied on the entrepreneurial or management efforts of others to realize an expectation of profit. *Id.*; *see also* APRIL 2019 GUIDANCE STATEMENT, *supra* note 23, at 5.

32. *See* LEWIS, *supra* note 30, at 278–79 (summarizing events leading up to Ethereum’s launch).

the value of those coins.<sup>33</sup> This classification may have persisted for some time, perhaps well after the network's launch one year later in July of 2015—since Buterin continued to be a vocal promoter and visible influence on the development of the network.<sup>34</sup> Nevertheless, as Director Hinman explained, the now-complete decentralization of the Ethereum network forces the conclusion that “current offers and sales of Ether are not securities transactions.”<sup>35</sup> In other words, the same pre-mined Ether coins that may have been securities when issued in the crowdsale and through the launch of the network, morphed into nonsecurities at that subsequent moment (however difficult to pinpoint) when the Ethereum network became “sufficiently decentralized” to fail the fourth prong of *Howey*.<sup>36</sup>

From the standpoint of insider trading regulation, the fact that a cryptocurrency can morph from security to nonsecurity based on the extent to which the network that supports it has become “sufficiently decentralized,” creates significant legal uncertainty for traders. Absent some clear, bright-lined guidance from the SEC on just when a network will be deemed “sufficiently decentralized” to render a cryptocurrency a nonsecurity (or vice versa),<sup>37</sup> traders are left guessing. Those traders who regulators or prosecutors later decide have guessed wrong may be surprised to find they face insider trading liability, fines, and prison time.

The picture still becomes more complicated when one compares pre-mined tokens issued in an ICO or initial crowdsale with those that are openly mined by network participants after the launch. Professors Todd Henderson and Max Raskin argue that openly mined coins may not be securities because they may fail the first prong of the *Howey* test, requiring the investment of

33. See Hinman, *Remarks*, *supra* note 24.

34. See, e.g., Joon Ian Wong & Ian Kar, *Everything You Need to Know About the Ethereum ‘Hard Fork’*, QUARTZ (July 18, 2016), <https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork> [<https://perma.cc/D2UT-YHTT>] (noting that Vitalik Buterin and his team played a visible role in finding a solution to the 2016 DAO hack).

35. Hinman, *Remarks*, *supra* note 24.

36. *Id.*

37. The April 2019 Guidance Statement does not offer such a clear test. It offers nothing more than a non-exhaustive multi-factor analysis for determining whether “a digital asset previously sold as a security should be reevaluated at the time of later offers or sales” as to whether it has morphed into a nonsecurity. APRIL 2019 GUIDANCE STATEMENT, *supra* note 23, at 5. The factors include, but are not limited to:

- Whether or not the efforts of an AP [Active Participant], including any successor AP, continue to be important to the value of an investment in the digital asset.
- Whether the network on which the digital asset is to function operates in such a manner that purchasers would no longer reasonably expect an AP to carry out essential managerial or entrepreneurial efforts.
- Whether the efforts of an AP are no longer affecting the enterprise's success.

*Id.* The last factor is particularly vague and unhelpful, since the conduct of a high-profile participant like Vitalik Buterin might *always* “affect” an enterprise such as Ethereum's subsequent success.

money.<sup>38</sup> With openly-mined coins, “there is an exchange not of money, but of computing resources, for the digital asset.”<sup>39</sup> The point is fair. It would seem that most people are unlikely to “invest” computer resources in the capital markets, and so there is little relation between the capital markets and those computer resources.<sup>40</sup> Moreover, even if one finds a miner’s expenditure of computer resources to be an “investment” that satisfies the first prong of *Howey*,<sup>41</sup> Henderson and Raskin suggest that openly mined coins should also “be considered *prima facie* sufficiently decentralized” to fail the fourth prong of the *Howey* test as well.<sup>42</sup> For, “when a token is openly mined, then there is no technical distinction between promoter and participator as both are on even footing. They are interacting with code that can only be changed through consensus.”<sup>43</sup>

This raises an additional concern for insider trading enforcement. Even if a recently-launched cryptocurrency is not sufficiently decentralized to morph pre-mined coins from securities into nonsecurities, should the openly mined coins on the same blockchain nevertheless be regarded as nonsecurities? Is the former to be regulated by the SEC and the latter not—despite the fact that they are identical in all other respects? Consequently, will it be permissible to insider trade coins that are openly mined, but criminal to affect the same trading in those that are pre-mined? Or is the mere fact that coins *are* being mined itself sufficient evidence of decentralization that all coins on the blockchain are nonsecurities under *Howey*?<sup>44</sup>

In addition, the “expectation of profit” prong of the *Howey* test as applied to cryptoassets can also be quite murky, particularly where tokens can be redeemed for products or services. Under the SEC Staff’s current guidance, market participants should consider no fewer than thirty-seven characteristics and sub-characteristics to determine whether there is a reasonable expectation of profit in a given digital asset.<sup>45</sup> Moreover, as with the “efforts of others” test outlined above, there is the possibility that a given token that is issued with the expectation of profits may later be offered and sold without such an expectation—and six non-exclusive factors are offered by the staff to

---

38. M. Todd Henderson & Max Raskin, *A Regulatory Classification of Digital Assets: Toward an Operational Howey Test for Cryptocurrencies, ICOs, and Other Digital Assets*, 2019 COLUM. BUS. L. REV. 443, 464 (2019).

39. *Id.*

40. The point here is not that the “investment of money” prong of the *Howey* test requires cash payment; clearly it does not. *See, e.g., Uselton v. Commercial Lovelace Motor Freight, Inc.*, 940 F.2d 564, 574 (10th Cir. 1991) (“[I]t is well established that cash is not the only form of contribution or investment that will create an investment contract.”).

41. *See Int’l Bhd. of Teamsters v. Daniel*, 439 U.S. 551, 560 n.12 (1979) (stating the investment may take the form of “goods and services”).

42. Henderson & Raskin, *supra* note 38, at 464.

43. *Id.* at 463.

44. *See id.* at 464 (“[A]ssets that are mined in an open process where anyone can participate should be considered *prima facie* sufficiently decentralized.”).

45. *See* APRIL 2019 GUIDANCE STATEMENT, *supra* note 23, at 6–10.

aid in this determination.<sup>46</sup> As some commentators have noted, “the trouble with [such] multi-factor analyses is that they create legal uncertainty,” though they may afford greater “flexibility to the regulator.”<sup>47</sup>

The Supreme Court has held that a criminal “conviction fails to comport with due process if the statute under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.”<sup>48</sup> Though the charge that insider trading law in the United States is unconstitutionally vague is nothing new,<sup>49</sup> when one combines the mysteries surrounding the law’s more traditional applications (summarized in Section II of this paper) with the above-referenced ambiguities that arise in the emerging context of cryptoassets, it is difficult to see how a person of ordinary intelligence is placed on fair notice of potential criminal liability in even fairly straightforward circumstances like the one offered in the introduction to this paper. Has the SEC offered sufficient guidance to place Cryptobase employees of ordinary intelligence on notice of whether their trades in Geekcoins incurred insider trading liability? How are they to determine with any certainty whether the Geekcoin network is sufficiently decentralized? Were they trading for minted or openly mined coins—and does this matter? Do those who trade in Geekcoins do so with a reasonable expectation of profits?

Finally, and perhaps more interesting and perplexing, note that any potential insider trading liability for Cryptobase employees in our example would have to be under the misappropriation theory—for Cryptobase employees have no obvious fiduciary or similar relation of trust and confidence with Geekcoin owners. Recall, however, that a breach of trust and confidence to the source of the information (in this case, Cryptobase) is crucial to liability under the misappropriation theory. In our example, however, Cryptobase management expressly authorized this trading—the information was not therefore obtained under false pretenses as is required for misappropriation liability under *O’Hagan*.<sup>50</sup> There would, therefore, be no grounds for misappropriation liability pursuant to established and controlling

---

46. See *id.* at 8.

47. Henderson & Raskin, *supra* note 38, at 478.

48. *United States v. Williams*, 553 U.S. 285, 304 (2008) (citing *Hill v. Colorado*, 530 U.S. 703, 732 (2000)).

49. See, e.g., Homer Kripke, *Manne’s Insider Trading Thesis and Other Failures of Conservative Economics*, 4 CATO J. 945, 949 (1985).

50. See *United States v. O’Hagan*, 521 U.S. 642, 643 (1997) (“Misappropriation, as just defined, is the proper subject of a § 10(b) charge because it meets the statutory requirement that there be ‘deceptive’ conduct ‘in connection with’ a securities transaction. First, misappropriators deal in deception: A fiduciary who pretends loyalty to the principal while secretly converting the principal’s information for personal gain dupes or defrauds the principal. A company’s confidential information qualifies as property to which the company has a right of exclusive use; the undisclosed misappropriation of such information constitutes fraud akin to embezzlement.”).



Supreme Court precedent.<sup>51</sup> This limitation of the scope of insider trading liability under the misappropriation theory has yet to be tested in an actual case or controversy before the courts. I suspect this is because, in light of the fact that ours is a vaguely defined common-law insider trading regime, most firms adopt “play-it-safe” insider trading compliance policies—and are prudent to do so.<sup>52</sup> However, given the current uncertainty over whether or when a cryptocurrency is a security at all, unwitting traders in digital assets may find this is the only defense available to them. Moreover, the cypherpunks<sup>53</sup> who compose many crypto-development teams seem to revel in creative exploitation of loopholes, and are notorious for challenging authority in an effort to improve electronic independence and privacy.<sup>54</sup> Consequently, the crypto-culture may be more willing to risk such a legal confrontation to preserve independence and avoid regulation. In any event, the expansion of the misappropriation theory to capture the conduct summarized in our example (where the trading is licensed by the CEO) would be a common-law extension of the current insider trading regime as defined in *O’Hagan*.<sup>55</sup> As such, it would be a violation of the principle of legality. Moreover, when one combines the vagueness that already plagues our insider trading enforcement regime with new uncertainties raised by its application to the still-nascent world of cryptoassets, I submit that it may also be an unconstitutionally vague application of Section 10(b).

---

51. *Id.* at 643–44 (“[F]ull disclosure forecloses liability: Because the deception essential to the theory involves feigning fidelity to the information’s source, if the fiduciary discloses to the source that he plans to trade on the information, there is no ‘deceptive device’ and thus no § 10(b) violation.”). Many have noted this limitation on misappropriation liability under the current regime. See John P. Anderson, *Anticipating a Sea Change for Insider Trading Law: From Trading Plan Crisis to Rational Reform*, 2015 UTAH L. REV. 339, 385–86 (2015); see also M. Todd Henderson, *Insider Trading and CEO Pay*, 64 VAND. L. REV. 505, 542–43 (2011); Saikrishna Prakash, *Our Dysfunctional Insider Trading Regime*, 99 COLUM. L. REV. 1491, 1515–20 (1999).

52. See, e.g., John P. Anderson, *Solving the Paradox of Insider Trading Compliance*, 88 TEMP. L. REV. 273, 273–311 (2016).

53. Cypherpunks are activists advocating for the use of cryptography and other technologies to protect privacy and effect social and political change in the digital age. See, e.g., Jameson Lopp, *Bitcoin and the Rise of the Cypherpunks*, COINDESK (April 9, 2016, 12:43 PM), <https://www.coindesk.com/the-rise-of-the-cypherpunks> [<https://perma.cc/2RDL-RGNW>]. The “cypherpunk” movement began with a mailing list in the late 1980s and 1990s. *Id.*

54. “Cypherpunks tended to be libertarian-leaning in the sense that they believed society would be better with minimal government. Cypherpunks believed one of the best ways to protect their interests was to remain anonymous and that ‘privacy in an open society requires [an] anonymous transaction system . . .’ like distributed ledger technology provides today. Rebecca K. Webster, *Challenges in Compensating Employees in Cryptocurrencies*, 39 MITCHELL HAMLINE L.J. PUB. POL’Y & PRAC. 157, 162 (2018); see also Lopp, *supra* note 53.

55. Even those who argue that existing insider trading laws unambiguously apply (and ought to apply) to informed trading in cryptoassets appear willing to concede that liability under the misappropriation theory is only triggered if the source of the information does not authorize the trading. See, e.g., Andrew Verstein, *Crypto Assets and Insider Trading Law’s Domain*, 105 IOWA L. REV. 1, 35 (2019) (noting that “permission to trade” from the source would preclude liability for a cryptoasset trader under the misappropriation theory).

## IV. CONCLUSION

The absence of any clear guidance on when a digital asset is a security is a problem that has ramifications far beyond this article's limited focus on our insider trading enforcement regime.<sup>56</sup> Nevertheless, I have argued that the impending application of our insider trading laws to cryptoassets helps to illustrate why it is unfair and unjust to force market participants to wait much longer for a definitive answer to the question of when a digital asset is a security.

It may be that cryptoassets are too hard to shoehorn into any existing categories and should be recognized as comprised by a whole new asset class,<sup>57</sup> and regulated by an entirely new statutory or self-regulatory authority. Alternatively, existing authorities, such as the SEC, CFTC, and IRS could issue clear rule-based guidance on when a cryptoasset is a security or commodity, and how it should be taxed.<sup>58</sup> For example, the Swiss financial regulator, FINMA, recently issued guidance on when digital assets are securities.<sup>59</sup>

In any event, as the Bharara Task Force on Insider Trading pursues its mandate to propose reforms that will bring greater clarity and precision to our insider trading enforcement regime, its members should not ignore the issues introduced by the emergence of trading in cryptoassets. While I have argued that cryptoassets create new ambiguities for an already vague body of law, I have also suggested that viewing our insider trading regime through the fresh lens of cryptoassets may also help to bring some resolution to debates (e.g., over the scope of misappropriation liability) that have persisted for decades.

---

56. See, e.g., Henderson & Raskin, *supra* note 38.

57. LEWIS, *supra* note 30, at 61.

58. Promising frameworks have already been proposed. See, e.g., Henderson & Raskin, *supra* note 38 (proposing two approaches to operationalizing the Supreme Court's *Howey* test for application to digital assets).

59. See *FINMA Publishes ICO Guidelines*, FINMA (Feb. 16, 2018), <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung> [<https://perma.cc/C6KP-SKZT>].