LEGAL RECOURSE FOR VICTIMS OF BLOCKCHAIN AND CYBER BREACH ATTACKS

MICHAEL CONKLIN[*]
BRIAN ELZWEIG[**]
LAWRENCE J. TRAUTMAN[***]

ABSTRACT

Reports of disruptive cyber breaches remain a daily occurrence. The costs to individuals, businesses, government, healthcare providers, and educational institutions are staggering. Policy makers and corporate management continue to struggle to find solutions to these problems. Complicating the cybersecurity technical and regulatory challenges is the rapid pace of technological change, which brings novel threats with the relatively recent explosion of blockchain-enabled and artificial intelligence applications. Existing legislation—and related case law—was not written with such technologies, actions, or behavior in mind, which has led to considerable uncertainty. Differences in regulatory jurisdiction, based on the actual ways in which these new technologies are utilized, often create novel uncertainties and difficult compliance issues. Now, the threat landscape has become even more complicated due to emerging developments in quantum computing, "an emerging field that promises to solve problems too complex for existing supercomputers."[1] How has legal recourse for victims of cybercrimes developed, and what are the likely future developments in recovery for such injuries?

This Article proceeds in eight parts. First, the authors describe the history and mechanics of blockchain technology. Second is an explanation of societal and corporate responsibility for data security. Third is a description of the current status of the escalating cyber threat. Fourth, the authors discuss regulation of blockchain technology. Fifth is coverage of quantum computing. Sixth is a discussion of national security considerations. Seventh, the authors explain potential legal liability for injury resulting from cyberattacks and blockchain

[*]Powell Endowed Professor of Business Law at Angelo State University.
[**]Associate Professor of Business Law and Research Fellow of the Askew Institute of Multidisciplinary Studies at the University of West Florida.
[***]Associate Professor of Business Law and Ethics at Prairie View A&M, Associate Professor at Texas A&M University School of Law (by courtesy), External Affiliate, Indiana University Bloomington, Ostrom Workshops in Data Management & Information Governance, and Cybersecurity & Internet Governance.

[1] Benjamin Katz & Eric Niler, *Nobel Awarded for Quantum Computing,* WALL ST. J., Oct. 5, 2022, at A3.

exploits. Finally, the authors consider how this Article will hopefully catalyze future research on these matters. In sum, this Article provides a valuable framework to assess the mostly overlooked and fast-evolving cybersecurity threats posed by blockchain attacks.

TABLE OF CONTENTS

I. BLOCKCHAIN IN BRIEF

A considerable amount of scholarship describes blockchain technology and its various uses deployed to date.[2] This Article will not attempt to replicate that here. Rather, it will provide a brief thumbnail description for readers new to the topic and provide a road map to additional sources in the footnotes for those who desire to learn more.[3]

---

[2] *See, e.g.*, Lawrence J. Trautman, *Bitcoin, Virtual Currencies and the Struggle of Law and Regulation to Keep Pace*, 102 MARQ. L. REV. 447 (2018), https://ssrn.com/abstract=3182867; Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. 1041 (2017), http://ssrn.com/abstract=2730983; Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 CONSUMER FIN. L.Q. REP. 232 (2016), http://ssrn.com/abstract=2786186.

[3] *See*, Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, *Blockchain Demystified* (Queen Mary Sch. of L., Legal Studies Research Paper No. 268/2017), December 20, 2017, https://ssrn.com/abstract=3091218; Christian Catalini & Joshua S. Gans, *Initial Coin Offerings and the Value of Crypto Tokens* (MIT Sloan Research Paper No. 5347-18, Rotman School of Management Working Paper No. 3137213), 2019; Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain* (Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16, 2019), April 20, 2019, https://ssrn.com/abstract=2874598; Shaanan Cohney, David A. Hoffman, Jeremy Sklaroff & David Wishnick, *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591 (2019), https://ssrn.com/abstract=3215345; Lin Cong & Zhiguo He, *Blockchain Disruption and Smart Contracts*, 32 REV. FIN. STUD. 1754 (2019); Sean Foley, Jonathan R. Karlsen & Talis J. Putnins, *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*, REV. FIN. STUD. (forthcoming), https://ssrn.com/abstract=3102645; John M. Griffin & Amin Shams, Is Bitcoin Really Un-Tethered? (October 28, 2019) (unpublished manuscript), https://ssrn.com/abstract=3195066; Gur Huberman, Jacob Leshno & Ciamac C. Moallemi, *Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System,*(Colum. Bus. Sch., Research Paper No. 17-92), September 30, 2020, https://ssrn.com/abstract=3025604; Maximilian Friedlmaier, Andranik Tumasjan & Isabell M. Welpe, *Disrupting Industries With Blockchain: The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures*, 2018 PROC. 51ST ANN. HAW. INT'L CONF. ON SYS. SCIS. 3517 (2017), https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/f03d6a03-6f81-4937-947d-9c2d0c47796e/content; Octavian Nica, Karolina Piotrowska & Klaus Reiner Schenk-Hoppé, *Cryptocurrencies: Economic Benefits and Risks* (Univ. of Manchester, FinTech

A. Mechanics of Blockchain

As a threshold matter, Aaron Wright and Primavera De Filippi provide a helpful definition: "The blockchain is a distributed, shared, encrypted-database that serves as an irreversible and incorruptible public repository of information. It enables, for the first time, unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority."[4] In sum, the blockchain is a useful data structure that "leverages hash functions and encryption to provide the security of information . . . ."[5] Trautman and Molesky have written:

Blockchain is a modification and conglomeration of existing technology and concepts. Michael Scott explains, "The blockchain is a testament to the power of a single cryptographic primitive – the hash function. Really nothing else is required, so if you can get your head around the hash function, you can understand the basics of the blockchain." Mr. Scott describes a hash by stating:

A cryptographic hash function takes one input and calculates one output. For example, for the input 'We hold these truths to be self-evident', the well known hash function SHA256 produces the output:

> 84ba74b2661c87470665a1a5f5ab526afcf266f8c5effb795bef2d25 14a8afd3
> For the slightly different input "we hold these truths to be self-evident" (note the lower case w), the output is
> 246160c031a4ddd9d940e931721fdec7e72087c8eccf5ea5621bb15 d22959c19
> The above examples provide information about hash functions. Mr. Scott writes:
> The output bears no obvious relationship to the input, indeed it looks completely random. A tiny change to the input produces a

---

Working Paper No. 2), October 26, 2017, https://ssrn.com/abstract=3059856; Marc Pilkington, *Blockchain Technology: Principles and Applications*, *in* RESEARCH HANDBOOK ON DIGITAL TRANSFORMATIONS 225 (F. Xavier Olleros & Majlinda Zhegu, eds., 2016), ; Max Raskin, The Law and Legality of Smart Contracts, 1 GEO. L. TECH. REV. 304 (2017), https://ssrn.com/abstract=2959166; Fahad Saleh, *Blockchain Without Waste: Proof-of-Stake*, 34 REV. FIN. STUD. 1156 (2021), https://ssrn.com/abstract=3183935; Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313 (2017), https://ssrn.com/abstract=2936294; Dirk Andreas Zetzsche, Ross P. Buckley, Douglas W. Arner & Linus Föhr, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, 63 HARV. INT'L L.J. (2019), https://ssrn.com/abstract=3072298 https://ssrn.com/abstract=3137213;

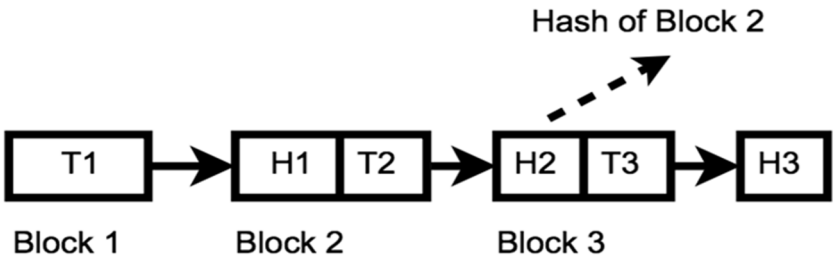
[4] Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and The Rise of Lex Cryptographia (revised July 25, 2017) (unpublished manuscript), https://ssrn.com/abstract=258 0664.

[5] Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, 88 UMKC L. REV. 239, 240 (2019), https://ssrn.com/abstract=3324660.

completely different output…. given just the output its impossible to determine the input. For this reason the hash function is often called a "one way" hash function. Also its impossible to find two different inputs which give the same output. For the function same length (actually 256 bits), independent of the length of the input.

Blockchain gets its names from the chaining of the hash. Mr. Scott provides us with a diagram appearing here as Exhibit 1.

Exhibit 1
A Simple Hash Chain



Mr. Scott writes the following explanation:

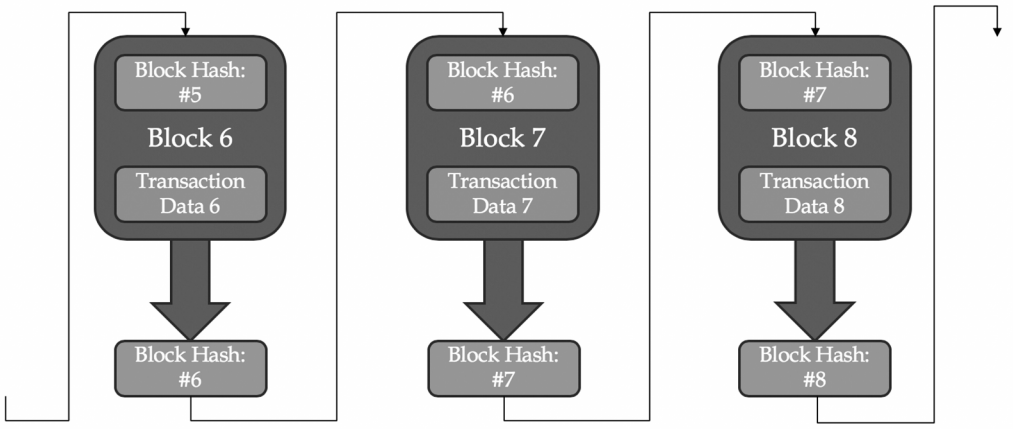
Here the T are "transactions" of some sort. Examine this diagram for a while, and appreciate the power of the chaining. The value H3 is calculated by hashing the whole of block 3, which includes the hash of block 2, which in turn includes the hash of block 1 etc. Note that because of the one-wayness of the hash function, this chain can only be calculated from left-to-right. So already we have some of the properties we want. This hash chain can potentially be used as an immutable record of transactions. Any attempt to tamper with it can be detected, as the hashes will change.

As Scott observes, "the term block comes a group of transactions. An important point – what we have described as individual

> transactions will probably consist in fact of a large batch of transactions all included inside of a single block."[6]

The process of a blockchain begins with transactional data being grouped together. Next, this data is combined with the hash of the previous block. Then, the hash for the current block is calculated by hashing the previous hash and the transaction data together. Finally, the process repeats by using this calculated hash for the next set of data. See Exhibit 2 below for a visual representation of this process.

Exhibit 2
Blockchain Hash Process



Source: Mason Molesky

B. Consensus Mechanism

What is called the consensus mechanism determines how and if the block will be accepted into the chain. These mechanisms can be based on a variety of factors in an attempt to provide assurances of truth, reliability, and validity of the information being added to the chain. In Bitcoin, this is done by solving a mathematical problem and rewarding the person who solves it first. Thus, entities are incentivized to correctly validate the data. This scheme is called "proof of work." Another popular consensus mechanism is called "proof of stake," in which entities stake currency or reputation in order to validate data. This again incentivizes entities to verify the correct set of data since currency or reputation can be lost. There are several other consensus mechanisms that exist and are under

---

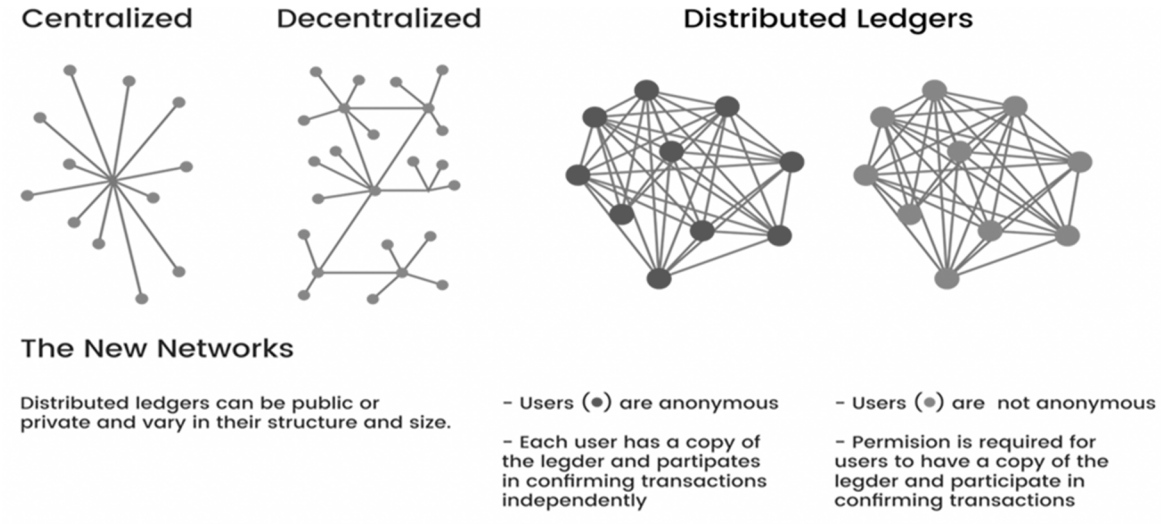
[6] *Id.* at 242–43 (quoting Michael Scott, *The Essence of the Blockchain*, MIRACL (2019), https://miracl.com/blog/the-essence-of-the-blockchain/).

research. One such mechanism, the practical Byzantine Fault Tolerance algorithm, is described and discussed in the research below.

C. Types of Blockchains (Digit Ledgers)

Blockchains can either be centralized or decentralized and can also be public or private. Please see Exhibit 3.

Exhibit 3[7]
Ledger Types



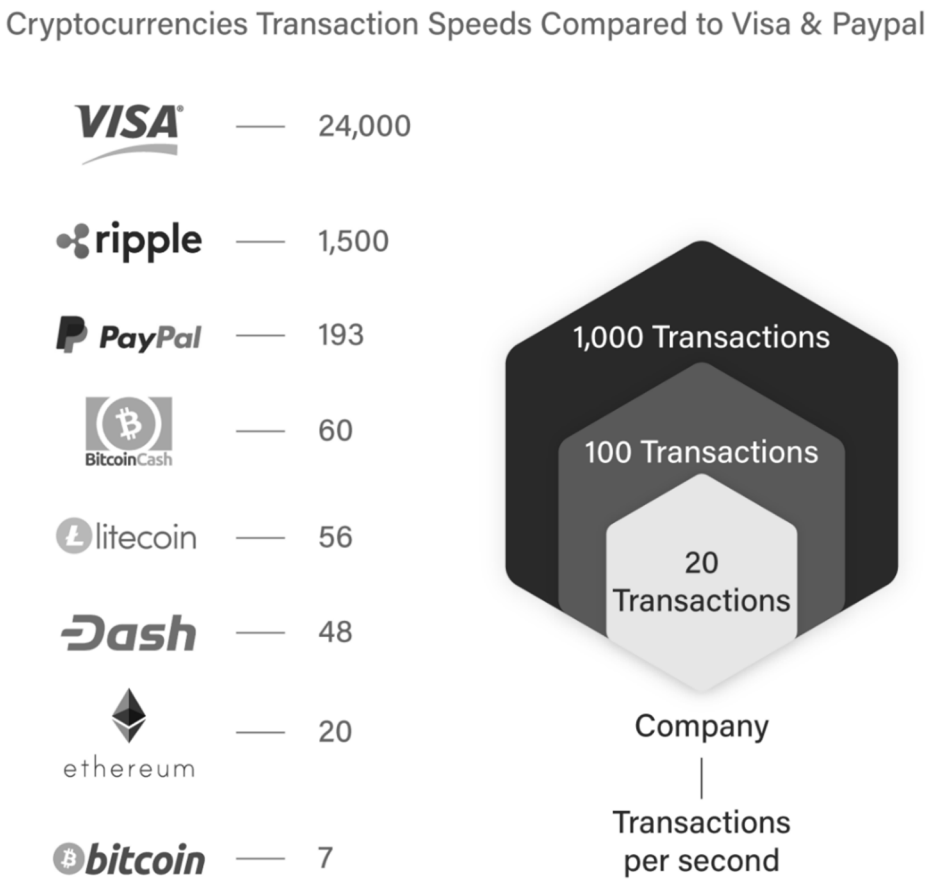
D. Challenges

The biggest problem that distributed ledger technologies face is scalability for adoption in the real world. Even cryptosystems like Bitcoin lack the scalability to be adopted in a way that largely replaces current systems. For example, as Bitcoin exists, it could not be adopted by a country or large bank to replace the existing online banking systems because of its limitation on the number of transactions that can be processed at a time and the prolonged time it takes to verify a transaction. A number of modifications have been developed to speed up the transaction and verification rate for Bitcoin, but these modifications are not enough for widespread use or adoption. An extensive overhaul of the Bitcoin protocols

[7] Aran Davies, *What is the Difference between Public vs Private Blockchain?*, DEVTEAM.SPACE, https://www.devteam.space/blog/public-vs-private-permissioned-blockchain-comparison/ (last visited Jan. 4, 2023).

would be necessary for it to function on a widespread system. This lack of scalability in the design of Bitcoin creates a challenge for realistic use because most blockchain technologies significantly lag behind established centralized financial systems like VISA.

Exhibit 5[8]
Transaction Speeds



II. RESPONSIBILITY FOR ENSURING DATA SECURITY

Maintaining defenses to cyber threats has proven to be particularly vexing for free societies, such as the United States.

[8] *A Deep Dive Into Blockchain Scalability*, CRYPTO.COM (Jan. 3, 2020), https://crypto.com/university/blockchain-scalability.

A. Societal Responsibility

In a democracy, all facets of society bear responsibility for maintaining effective cybersecurity. Indeed, it is the weakest link in the chain of connected devices—wherever located—that is typically responsible for a successful intrusion. Consider that "[t]he weakest link in security, as it's been since the Trojan War, is humans."[9] Christopher Mims explains, "the philosophy known as zero-trust architecture, assumes that no matter how robust a company's external defenses are, hackers can get in. So companies need to make sure that even users inside a network can't do serious damage."[10]

Professor and former director of research at the National Security Agency (NSA) Frederick R. Chang offers the following explanation:

> Basically, what directors need to know about cyber is that it is a strategic risk and not just an IT thing. It's easy to think of it as if there are some routers or some switches or some firewalls that get broken, resulting in exposed data—creating a problem. It's important to step back and reflect upon how cyber is a risk, like any other risk. It can be thought of like an earthquake, or a flood or a fire. Much like an earthquake, flood, or fire — you can't do anything about it if there's going to be an earthquake, and you are located in California. You can't stop the earthquake. All too often, it seems, there is a perception that cyber threat can actually be stopped. It can't be stopped. If a persistent attacker has a really high desire to break through, then they're going to get through. You can't stop them—and cyber has to be viewed as a risk, like any other risk[.] . . . [T]here are some things you can do to mitigate . . . the risk, but you can't eliminate the risk. Maybe you can buy insurance, you can bring in some more people to work on cybersecurity, and so forth. But cyber threat is fundamentally something you can't stop, and it needs to be viewed at that level. So, what steps does a board take to have enough intrinsic knowledge about cyber? The task can be a highly technical thing, but it isn't only a technical concern.[11]

---

[9] Christopher Mims, *Hackers Know… The Weakest Link is You*, WALL ST. J., Sept. 24–25, 2022, at B1.

[10] *Id.*

[11] Lawrence J. Trautman et al., *Corporate Directors: Who They Are, What They Do, Cyber and Other Contemporary Challenges*, 70 BUFF. L. REV. 459, 509 (2022), https://ssrn.com/abstract=3792382.

B. Corporate Governance

By late 2022, "[a] mix of regulation, investor demands and insurance requirements is pushing companies to elevate the oversight of cybersecurity, officials from the U.S. and other countries say."[12] Cybersecurity and Infrastructure Security Agency executive director Brandon Wales states, "While some companies in specific critical infrastructure sectors, such as energy and banking, must already comply with certain cybersecurity requirements, greater investment in digital defenses is needed across the board."[13]

C. Caremark and Progeny

The *Caremark* doctrine and corporate director liability for governance of cybersecurity have undergone dramatic change since 2019. Professors Pace and Trautman have recently written about how "the Supreme Court of Delaware reversed a decision by the Delaware Court of Chancery . . . dismissing a claim against the directors of Blue Bell Creameries, Inc. . . . under *Caremark*."[14] In sum:

> For decades, Chancellor Allen's description of a *Caremark* claim as "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment" held true. *Caremark* claims that survived a motion to dismiss was for decades few and far between. That changed in 2019. In the space of little over two years, Delaware courts have allowed five *Caremark* claims to survive a motion to dismiss. The thread holding that sword is beginning to look more like the single horsehair of myth . . . The scope and likelihood of *Caremark* liability are matters of considerable interest and concern for directors. Under most circumstances, a board simply doing its job poorly is relevant only to the directors' duty of care and protected by the business judgment rule, exculpatory provisions under Section 102(b)(7), and advancement and indemnification. Failure to monitor under *Caremark*, however, is a breach of the duty of loyalty. A breach of the duty of loyalty is not protected by the business judgment rule. It cannot be exculpated. And it cannot be covered by indemnification.

---

[12] James Rundle, *Investments in Cybersecurity Are No longer Optional, Officials Warn,* WALL ST. J., Sept. 22, 2022, at B4.

[13] *Id.*

[14] H. Justin Pace & Lawrence J. Trautman, *Mission Critical: Caremark, Blue Bell, and Director Responsibility for Cybersecurity Governance*, 2022 WIS. L. REV. 887, 890 (2022), http://ssrn.com/abstract=3938128.

> 2019 marked an abrupt shift in *Caremark* in application, if not in theory. In June of that year, the Delaware Supreme Court reversed a decision by the Chancery Court dismissing a claim against the directors of Blue Bell under *Caremark*. Within a little over a year, the Chancery Court would sustain *Caremark* claims in four cases. In *Clovis*, the Chancery Court sustained a *Caremark* claim against directors of a pharmaceutical company who allowed the company to misrepresent the clinical trial success of one of its three drugs. In *Hughes*, the Chancery Court sustained a *Caremark* claim against directors of a Chinese company incorporated in Delaware that suffered from severe and pervasive accounting issues. In *Chou*, the Chancery Court sustained a *Caremark* claim against directors of a large pharmaceutical company who allowed an indirect subsidiary to essentially operate a criminal enterprise. And in *Boeing*, the Chancery Court sustained a *Caremark* claim against directors of an airplane manufacturer who did not pay attention to safety issues . . . .
>
> Black letter *Caremark* doctrine has not changed, but it is newly reinvigorated and the risks of *Caremark* liability for directors is greater than just a few years ago. Future *Caremark* liability will be centered on failure to provide board-level oversight of mission critical risks. Cybersecurity is mission critical to effectively *all* large companies today.[15]

Pace and Trautman have explained that "[c]ybersecurity—encompassing data security, anti-hacking, data privacy, and more—has become just such a mission critical risk for large corporations."[16] Corporate boards are responsible for cybersecurity and directors are charged with a duty to ensure the corporation takes reasonable measures to protect corporate data.[17] In addition:

> This duty has legal teeth to it, including by federal and state statute. Personal liability for breaches of the duty of care, however, are of limited concern for directors because they are protected by the

---

[15] *Id.* at 888–90, 951.

[16] *Id.* at 891.

[17] Lawrence J. Trautman, *Managing Cyberthreat*, 33 SANTA CLARA HIGH TECH. L.J. 230 (2016), http://ssrn.com/abstract=2534119; *See also* Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, 13 HASTINGS BUS. L.J. 275 (2017), http://ssrn.com/abstract=2623219; Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment*, 11 FLA. ST. U. BUS. REV. 75 (2012), http://www.ssrn.com/abstract=1998489; Lawrence J. Trautman & Kara Altenbaumer-Price, *D&O Insurance: A Primer*, 1 AM. U. BUS. L. REV. 337 (2012), http://www.ssrn.com/abstract=1998080; Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?*, 11 DEPAUL BUS. & COMM. L.J. 205 (2013), http://www.ssrn.com/abstract=2137747 (discussing need for board cyber skills).

business judgment rule, corporate indemnification, and Section 102(b)(7) exculpatory provisions. The newly increased risk of *Caremark* liability drastically changes the landscape for potential liability because failure to properly monitor cybersecurity can violate the duty of loyalty.[18]

III. CYBERSECURITY THREAT ESCALATES

Reported cyberbreaches continue at an alarming rate.[19] As just one example of the seemingly daily announced breaches, *The Wall Street Journal* reports, "Uber Technologies Inc. said . . . that it was a victim of the group, called Lapsus$, saying it gained access to the company's internal systems and posted messages, including a graphic image, to employees."[20] Providing context, the report continues to note, "Last month, Cisco Systems Inc. said it had been hacked, most likely by a hacker affiliated with Lapsus$. And during a month-long rampage around March, the group broke into the networks of chip maker Nvidia Corp., Microsoft Corp., online access management vendor Okta Inc., Samsung Electronics Co., and others . . . ."[21] Within the same week, "Take-Two Interactive Software Inc. said hackers broke into the networks of its Rockstar Games Inc. unit and illegally accessed early-development footage of the company's next 'Grand Theft Auto' videogame."[22]

In 2021, the Federal Bureau of Investigation reported receiving "847,376 reports of cyberattacks . . . up 7% from 2020."[23] The literature is full of various depictions of the history and nature of cyber threats and breaches.[24]

---

[18] Pace & Trautman, *supra* note 17, at 894.

[19] Catherine Stupp, *Cyberattack Disrupts Global Hotel Group*, WALL ST. J., Sept. 27, 2022, at B4 (describing how cyberattack left "a trail of angry customers, lost income and a class-action lawsuit"); *see also* Lawrence J. Trautman, Scott Shackelford, Brian Elzweig & Peter C. Ormerod, Cyber Threats to Business: Identifying and Responding to Digital Attacks (Nov. 3, 2022) (unpublished manuscript), https://ssrn.com/abstract=4262971.

[20] Robert McMillan, *Uber Says Collective Carried Out Hack*, WALL ST. J., Sept. 21, 2022, at B1.

[21] *Id.*

[22] Sabela Ojea, *Take-Two Says Hackers Leaked Game Footage*, WALL ST. J., Sept. 20, 2022, at B4.

[23] Catherine Stupp, *After Prison, Hackers Face Tech Barriers*, WALL ST. J., Sept. 22, 2022, at B5.

[24] *See, e.g.*, Mohammed T. Hussein & Lawrence J. Trautman, The Internet of Things (IoT) in a Post-Pandemic World (July 18, 2022) (unpublished manuscript), http://ssrn.com/abstract=4149477; Lawrence J. Trautman, *Rapid Technological Change and U.S. Entrepreneurial Risk in International Markets: Focus on Data Security, Information Privacy, Bribery and Corruption*, 49 CAP. U. L. REV. 67 (2021), https://ssrn.com/abstract=2912072; Lawrence J. Trautman, Mohammed T. Hussein, Emmanuel U. Opara, Mason J. Molesky and Shahedur Rahman, *Posted: No Phishing*, 8 EMORY CORP. GOV. & ACCT. REV. 39 (2021), http://ssrn.com/abstract=3549992; Lawrence J. Trautman, Mohammed T. Hussein, Louis Ngamassi & Mason Molesky, *Governance of The Internet of Things (IoT)*, 60 JURIMETRICS 315 (2020), http://ssrn.com/abstract=3443973; David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability*, 18 COL. TECH. L.J. 49 (2020), http://ssrn.com/abstract=3251479; Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis*, 20 PITT. J. TECH. L. & POL'Y 41 (2020), http://ssrn.com/abstract=3363002; Lawrence J.

A. Blockchain "Bridge" Vulnerabilities and Attacks

On October 8, 2022, *The New York Times* reported that "Binance, the world's biggest cryptocurrency exchange, confirmed . . . that $570 million had been stolen in a hack of a blockchain it runs that serves as a bridge for asset transfers between networks."[25] The *Times* report warned:

> The attack on the Binance Smart Chain network highlighted weaknesses in decentralized finance, or DeFi, where transactions are controlled by code.
> 'Software code is never bug free,' Binance's chief executive, Changpeng Zhao, said in an interview with CNBC. He emphasized that no users had lost money in the hack but said that so-called cross-chain bridges were particularly vulnerable to hacks and the industry needed to get better at learning from them. 'We have seen a series of attacks on targeting vulnerabilities in cross-chain bridges,' Binance Smart Chain wrote in a blog post apologizing to users. "We will openly share the details of the postmortem and all lessons on how to implement more advanced security measures to shore-up these vulnerabilities."
> In August, the blockchain research company Chainalysis estimated that $2 billion worth of cryptocurrency had been stolen in 13 cross-chain bridge attacks, mostly in 2022. In March, an attack drained $600 million from a bridge behind the crypto-powered video game Axie Infinity. In February, $325 million was stolen from the Wormhole network. These exploits show that a reliance on code for control of DeFi platforms leaves these systems exposed, and that in emergency situations, decentralization can be an obstacle to quickly resolving issues. The Binance chain ecosystem is run by a community of users, known as validators, who hold tokens and can vote on proposed code changes. 'Decentralized chains are not designed to be stopped, but by contacting community validators

---

Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503 (2019), http://ssrn.com/abstract=3238293; Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761 (2018), http://ssrn.com/abstract=2982629; Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-Commerce, Political and Regulatory Compliance Risks*, 10 WM. & MARY BUS. L. REV. 1 (2018), https://ssrn.com/abstract=3067298; Lawrence J. Trautman, *E-Commerce, Cyber and Electronic Payment System Risks: Lessons from PayPal*, 16 U.C. DAVIS BUS. L.J. 261 (2016), http://www.ssrn.com/abstract=2314119; Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works*, 5 J.L. & CYBER WARFARE 147 (2016), http://ssrn.com/abstract=2638448; Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341 (2015), http://ssrn.com/abstract=2548561.

[25] Ephrat Livni, *Binance Is Hit by a $570 Million Hack*, N.Y. TIMES, Oct. 8, 2022, at B4.

> one by one, we were able to stop the incident from spreading,' Binance Smart Chain said in its statement. 'This delayed closure, but we were able to minimize the loss.'
> Now, the Binance Smart Chain community will hold a vote on next steps, including whether to freeze the stolen funds and allot a bounty for catching the hackers, offering up to 10 percent of the value of the stolen assets. Vitalik Buterin, one of the founders of the Ethereum network — and the second-most-popular cryptocurrency, Ether — has been a vocal critic of cross-chain bridges, noting that they have "fundamental security limits."[26]

IV. REGULATION OF BLOCKCHAIN TECHNOLOGY

In a global economy and internet-connected world, the effective regulation of blockchain technology is a challenging and complicated process, involving multiple international regulatory authorities.[27]

A. The SEC's History of Blockchain Regulation

The Securities and Exchange Commission (SEC) has been granted broad authority to regulate securities in the United States. The SEC has been given authority to regulate both the initial offering of securities[28] and ongoing

---

[26] *Id.*

[27] Stéphane Blemus, *Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide*, REVUE TRIMESTRIELLE DE DROIT FINANCIER, Dec. 2017, https://ssrns.com/abstract=3080639; Joanna Caytas, *Developing Blockchain Real-Time Clearing and Settlement in the EU, U.S., and Globally*, COLUM. J. EURO. L.: PRELIMINARY REF. (June 22, 2016), http://cjel.law.columbia.edu/preliminary-reference/2016/developing-blockchain-real-time-clearing-and-settlement-in-the-eu-u-s-and-globally-2/; Sean S. Cao, Lin Cong & Baozhong Yang, Financial Reporting and Blockchains: Audit Pricing, Misstatements, and Regulation (June 26, 2019) (unpublished manuscript), https://ssrn.com/abstract=3248002; Philipp Hacker & Chris Thomale, *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies Under EU Financial Law*, 15 EURO. CO. & FIN. L. REV. 645 (2018), https://ssrn.com/abstract=3075820; Hossein Kakavand, Nicolette Kost De Sevres & Bart Chilton, The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies (Jan. 1, 2017) (unpublished manuscript), https://ssrn.com/abstract=2849241;;Juliet M. Moringiello & Christopher K. Odinet, *The Property Law of Tokens*, 74 FLA. L. REV. 607 (2022), https://ssrn.com/abstract=3928901; Philipp Paech, *The Governance of Blockchain Financial Networks*, 80 MODERN L. REV. 1073 (2017), https://ssrn.com/abstract=2875487; Gareth Peters, Efstathios Panayi & Ariane Chapelle, *Trends in Cryptocurrencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective*, J. FIN. PERSPECTIVES, Winter 2015, https://ssrn.com/abstract=3084011; Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox*, 3 GEO. L. TECH. REV. 281 (2019), https://ssrn.com/abstract=3193576;Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 489 (2018), https://ssrn.com/abstract=2844409.

[28] 15 U.S.C. § 77.

transactions in the sale and purchases of securities.[29] However, the SEC's power is relegated only to securities, so if an asset does not meet the definition of a security, the SEC will not have regulatory authority over that asset. There is confusion regarding whether and when digital assets meet the criteria to be considered a security.[30] The lack of clarity, at least in part, can be attributed to the SEC regulating through enforcement actions rather than enacting specific regulations regarding cyber assets.

Innovation occurring within the digital asset markets is outpacing the ability for the SEC to enact regulations.[31] The SEC has been given scant guidance and has been inconsistent regarding when a digital asset must be registered as a security.[32] The term "security" is defined in the Securities Act of 1933 (Securities Act) as:

> any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.[33]

---

[29] 15 U.S.C. § 78.

[30] *See* Carol R. Goforth, *Regulation of Crypto: Who Is the Securities and Exchange Commission Protecting?*, 58 AM. BUS. L.J. 643, 645–46. (2021).

[31] *Id.* at 645; *see also* Neal Newman & Lawrence J. Trautman, *Special Purpose Acquisition Companies (SPACs) and the SEC*, 24 U. PA. J. BUS. L. 639 (2022) (discussing NFTs), http://ssrn.com/abstract=3905372; Neal Newman & Lawrence J. Trautman, *Securities Law: Overview and Contemporary Issues*, 16 OHIO ST. BUS. L.J. 149 (2021), http://ssrn.com/abstract=3790804; Lawrence J. Trautman & George P. Michaely, Jr., *The SEC & The Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L. Q. REP. 262 (2014), http://www.ssrn.com/abstract=1951148; Lawrence J. Trautman & Neal Newman, *A Proposed SEC Cyber Data Disclosure Advisory Commission*, 50 SEC. REG. L.J. 199 (2022), http://ssrn.com/abstract=4097138.

[32] Brian Elzweig & Lawrence Trautman, *When Does a Nonfungible Token (NFT) Become a Security?*, 39 GA. ST. U. L. REV. (forthcoming).

[33] 15 U.S.C. § 77b.

In terms of digital assets, to be a security, the asset would have to be an investment contract.[34] However, the Securities Act does not define the term investment contract.[35] Instead, the term was defined by the Supreme Court in *Securities & Exchange Commission v. W. J. Howey Co.*[36] The Court in *Howey* determined that a sale of portioned shares of citrus groves in Florida, coupled with a contract for the seller to cultivate, market, and remit the net proceeds to the investor, was an investment contract, subject to the Securities Act.[37] In doing so, the Court, in 1946, defined the term "investment contract" by creating what is now known as the *Howey* Test.[38] The Court held that to determine whether a transaction is an investment contract, "the test is whether the scheme involves an investment of money in a common enterprise with profits to come solely from the efforts of others."[39] Modern courts have expanded the *Howey* Test to allow for transactions that involve exchanges of consideration other than money[40] and to allow for small amounts of investor efforts in deriving profits from an investment.[41] Courts generally interpret the *Howey* Test as requiring four elements: "(i) there is an investment of money (or something else of value); (ii) in a common enterprise; (iii) where the purchaser expects to receive profits; and (iv) the expectation of profits is from the essential entrepreneurial efforts of others."[42]

The position of both the SEC and the courts is that the *Howey* Test is the standard for determining whether a transaction is an investment contract. Unfortunately, the *Howey* Test does not provide specific guidance for sellers to determine whether a crypto asset is a security. In 2017, the SEC used the *Howey* Test to determine that a cryptocurrency may be a security in the *DAO Report*.[43] The DAO at issue there was a decentralized autonomous organization (from which it derived the name DAO) "embodied in computer code and executed on a distributed ledger or blockchain"[44] created by the software company Slock.it. Slock.it created DAO Tokens,[45] The holders of the DAO Tokens would be given investment options, and the investments were screened by Curators, who worked for Slock.it.

---

34 Goforth, *supra* note 33, at 648.

35 *Id.*

36 SEC v. W. J. Howey Co., 328 U.S. 293 (1946).

37 *Id.* at 294.

38 Goforth, *supra* 30, at 648–49.

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

40 Uselton v. Com. Lovelace Motor Freight, Inc., 940 F.2d 564, 574 (10th Cir. 1991).

41 *See, e.g.*, Sec. & Exch. Comm'n v. Glenn W. Turner Enters., Inc., 474 F.2d 476, 483 (9th Cir. 1973); Sec. & Exch. Comm'n v. Koscot Interplanetary, Inc., 497 F.2d 473, 480 (5th Cir. 1974).

42 Goforth, *supra* note 33, at 649 (citations omitted).

43 U.S. SEC. & EXCH. COMM'N, RELEASE NO. 81207, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO (2017) [hereinafter DAO REPORT], http://www.sec.gov/litigation/investreport/34-81207.pdf.

44 *Id.* at 1.

45 *Id.* at 4-5.

These Curators at Slock.it arranged an initial coin offering (ICO) of DAO Tokens worth approximately $150 million

In applying the *Howey* Test to Slock.it's DAO Tokens, the SEC relied on *SEC v. Shavers*, which held that digital currencies could be money, meeting the first prong of *Howey*.[46] In the *DAO Report*, the SEC did not address the second prong of the *Howey* Test, which requires investment in a common enterprise.[47] This was likely because commonality was clear, due to the pooling of the investments, with investors voting to reinvest or distribute those profits.[48] Commonality is easily met in an ICO that is not based on a non-profit, open-source network.[49] The third prong of the *Howey* test, requiring that investors have a reasonable expectation of profit, was easily met. Slock.it, in marketing the DAO, stated that the DAO was a "for-profit entity" with the objective to "fund projects in exchange for a return on investment."[50] The SEC also found that the final prong of the *Howey* Test, requiring profits be derived primarily from the managerial efforts of others, was met.[51] The SEC found that Slock.it's marketing kept active engagement in the DAO, and the use of Curators vetting the investment opportunities was essential to the success of the enterprise.[52]

Even though the SEC found that all the elements of the *Howey* Test were met, the SEC did not refer Slock.it or the DAO for enforcement. Instead, the SEC issued the *DAO Report* as an investigative report under section 21(a) of the Securities Exchange Act of 1934.[53] The *DAO Report* was seen as a warning to issuers of cyber tokens that the use of digital technology obfuscates the need to comply with securities registration laws.[54] The *DAO Report* established that failure to follow the guidance given in the report and securities registration requirements would lead to SEC enforcement actions.[55]

Soon after the *DAO Report*, the SEC's Enforcement Division created a Cyber Unit to target cyber-related misconduct, including "[v]iolations involving distributed ledger technology and initial coin offerings."[56] Initially, the SEC seemed to indicate that it was taking the position that all crypto assets were

---

46 DAO REPORT, *supra* note 46, at 11.
47 Elzweig & Trautman, *supra* note 35.
48 *Id.*
49 Mendelson, *supra* note 52, at 75.
50 DAO REPORT, *supra* note 36, at 11.
51 *Id.*
52 *Id.* at 12.
53 *Id.* at 1.
54 Mendelson, *supra* note 52, at 68–69.
55 Elzweig & Trautman, *supra* note 35.
56 Press Release, U.S. Sec. & Exch. Comm'n, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176.

securities.[57] Within a month of creating its Cyber Unit, the SEC brought its first enforcement action, using the *Howey* Test to determine that a MUN token issuance by Munchee, Inc., was an issuance of securities.[58] However, within a year of the *DAO Report*, William Hinman, who was then the director of the SEC's Division of Corporation Finance, stated that Bitcoin and Ether, two of the most widely used digital currencies, were not securities.[59] Hinman's statement seemed to rely on the lack of a common enterprise when it came to these digital currencies. Hinman stated, "[W]hen I look at Bitcoin today, I do not see a central third party whose efforts are a key determining factor in the enterprise. The network on which Bitcoin functions is operational and appears to have been decentralized for some time, perhaps from inception."[60] Hinman further noted that "putting aside the fundraising that accompanied the creation of Ether, based on [his] understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether are not securities transactions."[61] Hinman seemed to carefully craft the language about Ether currently not being a security, noting that the fundraising that accompanied Ether's creation was not part of his analysis.[62] Hinman instead commented that the nature of what is a security is not static and does not adhere to the instrument. Instead, a digital asset that was offered as a security may later become something other than a security.[63] This could occur when there is no central enterprise in the investment after the ICO.[64] Also, if a digital asset is a fully functional utility token only used to purchase goods or services on a decentralized network, it would not be a security.[65]

After calls for clarity, in 2018, the SEC issued guidance as to when a digital asset is a regulatable security in its *Framework for "Investment Contract" Analysis of Digital Assets* (*Framework*).[66] The *Framework* broke *Howey*'s five prongs into a series of thirty-eight factors to consider if the *Howey* Test was met. Instead of bringing clarity, many saw the *Framework* as bringing more confusion as to

---

[57] Goforth, *supra* note 33, at 650.

[58] Munchee Inc., Securities Act Release No. 10445, 118 SEC Docket 975 (Dec. 11, 2017).

[59] William Hinman, Dir., Div. of Corp. Finance, Sec. & Exch. Comm'n, Digital Asset Transactions: When Howey Met Gary (Plastic) (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] Andrew Bull & Tyler Harttraft, *Cryptocurrency and Blockchain Law: Sec's Heightened Enforcement Against Digital Assets*, 27 RICH. J.L. & TECH. 1, 29 (Aug. 2021).

[64] *Id.*

[65] *Id.*; *see also* Hinman, *supra* note 62.

[66] STRATEGIC HUB FOR INNOVATION & FIN. TECH., SEC. & EXCH. COMM'N, FRAMEWORK FOR "INVESTMENT CONTRACT" ANALYSIS OF DIGITAL ASSETS (2019) [hereinafter FRAMEWORK], https://www.sec.gov/files/dlt-framework.pdf.

whether a digital asset is a security.[67] Even then SEC Commissioner Hester Price noted:

> While Howey has four factors to consider, the framework lists 38 separate considerations, many of which include several sub-points. A seasoned securities lawyer might be able to infer which of these considerations will likely be controlling and might therefore be able to provide the appropriate weight to each . . . . [N]on-lawyers and lawyers not steeped in securities law and its attendant lore will not know what to make of the guidance.[68]

After the *Framework* was issued, the SEC focused its enforcement efforts pertaining to digital assets on ICOs.[69] In cases such as *SEC v. Kik*,[70] *SEC v. Telegram*,[71] and *SEC v. Ripple*,[72] "the SEC has been using litigation with fact specific inquiries to enforce its regulations on digital assets" to determine if the issuance of a digital currency was a security.[73] In *Ripple*, the SEC alleged that the ongoing trading of its XRP digital currency also constituted sales of securities because all of its XRP was already mined by Ripple (who originally owned all XRP), and Ripple would release more over time.[74] All three defendants claimed that the issuances did not result in profit from a common enterprise as required under *Howey*.[75] Confusion has been created by the SEC's regulation by enforcement, under which no clear guidance is provided as to when a digital asset needs to be registered as a security. Kik's general counsel advocated for the SEC to clarify its positions on the issuance of digital currency by regulation, stating, "[The SEC] should engage in proper rulemaking, including the opportunity for public commentary, rather than force our industry to hunt for regulatory clues among the SEC's conflicting statements, Commissioner and staff speeches, no-action letters, closed-door meetings with the SEC and nonprecedential

---

67 Elzweig & Trautman, *supra* note 35.

68 Hester M. Peirce, Comm'r, U.S. Sec. & Exch. Comm'n, How We Howey (May 9, 2019), https://www.sec.gov/news/speech/peirce-how-we-howey-050919.

69 Elzweig & Trautman, *supra* note 35.

70 U.S. Sec. & Exch. Comm'n v. Kik Interactive Inc., 492 F. Supp. 3d 169, 183 (S.D.N.Y. 2020).

71 Sec. & Exch. Comm'n v. Telegram Grp. Inc., 448 F. Supp. 3d 352, 358 (S.D.N.Y. 2020).

72 Complaint, Sec. & Exch. Comm'n v. Ripple Labs, Inc., No. 20-CV-10832 (S.D.N.Y. Dec. 22, 2020).

73 Jacqueline Hennelly, *The Cryptic Nature of Crypto Digital Assets Regulations: The Ripple Lawsuit and Why the Industry Needs Regulatory Clarity*, 27 FORDHAM J. CORP. & FIN. L. 259, 262 (2022).

74 Id. at 271–72.

75 *See generally* Goforth, *supra* note 33.

settlements."[76] This request for regulatory clarity has so far been unheeded. Instead, the SEC is continuing its strategy of using current regulations and enforcement to police cyber assets. In 2022, the SEC renamed its enforcement Cyber Unit, the Crypto Assets and Cyber Unit, and nearly doubled its size.[77] In its announcement, the SEC noted that since its creation in 2017, the Cyber Unit has brought more than eighty enforcement actions for unregistered and fraudulent crypto offerings and platforms.[78] In addition to the public calls for the SEC to implement a better regulatory regime to clarify when a cryptocurrency should be treated as a security, SEC Commissioner Mark Uyeda has echoed this call.[79] Uyeda stated:

> Today, one big, difficult, and complex issue that is conspicuously absent from the Commission's published regulatory agenda is how to regulate crypto assets and related services. Market participants have expressed significant concerns regarding the lack of regulatory guidance in this space. There is a widespread concern that the lack of predictability with regard to our regulation may encourage crypto firms to relocate to other jurisdictions.[80]

Uyeda noted that the lack of regulation creates uncertainty in determining whether a crypto asset is a security and, if so, how the industry complies with federal securities laws and SEC rules.[81] Uyeda opined that regulation by enforcement omits public comment and that without it "the Commission is unable to consider their perspectives in developing an appropriate regulatory framework. To the extent that crypto assets raise unique issues not otherwise addressed in the current rule book, the Commission should consider proposing rules or issuing interpretive releases."[82]

SEC Chair Gary Gensler disagrees with Uyeda's opinion and believes that the already enacted securities laws are sufficient to regulate crypto assets.[83] Gensler noted that the "vast majority" of tokens in the crypto market are securities, although the small number of tokens that are not securities may be a large part of the overall

---

[76] Nikhilesh De, Judge Rules Kik's Token Sale Violated US Securities Law, COINDESK (Sept. 14, 2021, 6:02 AM), https://www.coindesk.com/markets/2020/09/30/judge-rules-kiks-token-sale-violated-us-securities-law/.

[77] Press Release, U.S. Securities and Exchange Commission, SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit (May 3, 2022), https://www.sec.gov/news/press-release/2022-78.

[78] *Id.*

[79] Mark T. Uyeda, Comm'r, U.S. Sec. & Exch. Comm., Remarks at the "SEC Speaks" Conference 2022 (Sep. 9, 2022), https://www.sec.gov/news/speech/uyeda-speech-sec-speaks-090922.

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n, Speech "Kennedy and Crypto" (Sep.8, 2022), https://www.sec.gov/news/speech/gensler-sec-speaks-090822.

value of the market.[84] Gensler noted that the *Howey* Test is sufficient to determine when a crypto asset is a security, stating, "Without prejudging any one token, most crypto tokens are investment contracts under the *Howey* Test."[85] In response to calls for greater guidance, Gensler believes it has been clearly given "through the DAO Report, the Munchee Order, and dozens of Enforcement actions, all voted on by the Commission."[86]

Unless there is a policy shift within the SEC, it appears that its strategy will remain regulation through enforcement. The small number of non-security tokens referred to by Gensler would include tokens, such as Bitcoin, that do not have a centralized organization issuing the token. This would leave *Howey* unfulfilled because there is not a common enterprise in which profits are derived primarily from the efforts of another. However, Gensler did indicate that intermediaries (whether centralized or decentralized) "often are an amalgam of services that typically are separated from each other in the rest of the securities markets: exchange functions, broker-dealer functions, custodial and clearing functions, and lending functions."[87] This is reflected in the SEC's action for insider trading against Ishan Wahi, a manager for Coinbase's Assets and Investing Products, a crypto asset trading platform.[88] Although Coinbase claims that it does not list securities, in the Complaint, the SEC alleged that several listings on Coinbase were "crypto asset securities" meeting the definition of an investment contract.[89] Wahi allegedly tipped off his brother and a friend about the timing and content of the listing announcements of these assets.[90] For the SEC to be successful in this action, the SEC would have to prove its allegation that the listed investments were investment contracts under *Howey*. *Wahi* is an example of the SEC continuing its policy of regulation through enforcement actions, not only in the determination of whether an asset is a security but also in the ongoing trading of securities. This remains the SEC's strategy in lieu of creating new regulations specifically aimed to determine whether cyber tokens are securities, giving more certainty in their issuance.

B. Virtual Currencies

Significant global development of digital currencies has developed in just the past decade. Because of perceived anonymity, considerable initial use was in the advancement of illegal activities and purchases.[91] As early as "2013, the U.S.

---

84 *Id.*
85 *Id.*
86 *Id.*
87 *Id.*
88 Complaint, Sec. & Exch. Comm'n v. Wahi, No. 2:22-cv-01009 (E.D. Wash. July 21, 2022).
89 *Id.* at 7.
90 *Id.* at 1.
91 Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?* 20 RICH. J. L. & TECH. 13, 7–9 (2014), http://www.ssrn.com/abstract=2393537;

Treasury Department evoked the first use of the 2001 Patriot Act to exclude virtual currency provider Liberty Reserve from the U.S. financial system."[92] Fast-forward to late 2022, and the U.S. Department of Justice (DOJ) announced the deployment of "more than 150 federal prosecutors across the country to bolster law enforcement's efforts to combat the rise in crime linked to the use of cryptocurrencies."[93] *The Wall Street Journal* reports that DOJ's Digital Asset Coordinating Network is

> motivated in part because of the high degree of technical expertise that can go into prosecuting cryptocurrency cases, as well as digital currencies' increasing popularity across several different areas of crime, said Eun Young Choi, the first director of the Justice Department's national cryptocurrency enforcement team. Those areas include money laundering or financing terrorism, a vehicle of payment for ransomware hackers, and direct target of theft, she said.[94]

C. When Is an NFT a Security?

In a very short period of time, considerable scholarship has covered the topic of non-fungible tokens (NFTs).[95] Similar to other digital assets, the SEC has not given explicit guidance on when an NFT would qualify as a regulatable security.[96] Instead, issuers of NFTs will have to rely on the *Howey* Test to determine whether the issuance is a security.[97] *Howey* states that in an investment contract analysis, "[f]orm [must be] disregarded for substance and emphasis was

---

Lawrence J. Trautman, *Following the Money: Lessons from the "Panama Papers," Part 1: Tip of the Iceberg*, 121 PENN. ST. L. REV. 807, 847 (2017), http://ssrn.com/abstract=2783503.

[92] Trautman, *Virtual Currencies*, *supra* note 94, at 1 (first citing Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, § 224, 115 Stat. 272, 295; then citing Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't,* 97 NW. U. L. REV. 607 (2003), http://ssrn.com/abstract=317501; and then citing Press Release, Department of Justice, Co-founder of Liberty Reserve Pleads Guilty to Money Laundering in Manhattan Federal Court, (Oct. 31, 2013), http://www.justice.gov/opa/pr/2013/October/13-crm-1163.html).

[93] Dustin Volz, *Justice Department Forms National Network of Prosecutors Focused on Crypto Crime*, WALL ST. J., Sept. 17–18, 2022, at A4.

[94] *Id.*

[95] *See, e.g.*, Joshua Fairfield, *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, 97 IND. L.J. 1261 (2021); De-Rong Kong & Tse-Chun Lin, Alternative Investments in the Fintech Era: The Risk and Return of Non-fungible Token (NFT) (Aug. 30, 2021) (unpublished manuscript), https://ssrn.com/abstract=3914085; Edward Lee, *NFTs as Decentralized Intellectual Property*, 2023 U. ILL. L. REV. (2023), https://ssrn.com/abstract=4023736.

[96] See Elzweig & Trautman, *supra* note 35.

[97] *Id.*

placed upon economic reality."[98] This economic reality test means that NFTs must be analyzed on a case-by-case basis to determine whether they meet the definition of an investment contract.[99] The first prong of the *Howey* test is easily met, as all that is required is an exchange for something of value.[100] Traditional non-fractionalized NFTs are likely to fail the second prong of the *Howey* test, which requires that the NFT be part of a common enterprise. Unlike typical crypto assets, NFTs, by definition, are not fungible.[101] Most common NFTs represent a unique commodity, such as a piece of art, music, or video.[102] If an NFT representing a commodity is sold, generally, there are no further ties between the buyer and the seller in that transaction.[103] Further, there is a pooling of assets between the owner and other investors in the transaction.[104] Fractional NFTs (F-NFTs), however, are likely to become fungible.[105] Similar to traditional NFTs, F-NFTs represent a commodity, but as the name suggests, the ownership of the commodity is fractionalized.[106] The fractionalized shares (referred to as shards) can then be sold to multiple people, who become part owners of the F-NFT.[107] The fractionalization of the NFT takes a non-fungible asset and makes it fungible.[108] Once the shards are sold, F-NFTs often become investment vehicles, with the shard owners' fortunes tied to each other.[109] Commonality is also often met in F-NFTs because the sellers of the shards retain control of the NFT, intertwining the fortunes of the buyers with those of the seller.[110]

---

98 *W. J. Howey Co.*, 328 U.S. at 298.

99 Bull & Harttraft, *supra* note 66, at 14.

100 Goforth, *supra* note 33, at 649.

101 *See* Robert Anello, *Digital Art May Be Next in the SEC's Crosshairs*, FORBES (Jul. 15, 2021, 9:48 PM), https://www.forbes.com/sites/insider/2021/07/15/digital-art-may-be-next-in-the-secs-crosshairs/?sh=86602dc32dff [https://perma.cc/R5CP-9D89].

102 *Id.*; *see also* Lawrence J. Trautman, *Virtual Art and Non-fungible Tokens*, 50 HOFSTRA L. REV. 361 (2022), http://ssrn.com/abstract=3814087.

103 Robert Conti & John Schmidt, *What Is an NFT? Non-Fungible Tokens Explained*, FORBES (Apr. 8, 2022, 8:36 AM), https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/.

104 Revak v. SEC Realty Corp., 18 F.3d 81, 87 (2d Cir. 1994) (quoting Hart v. Pulte Homes of Mich. Corp., 735 F.2d 1001, 1004 (6th Cir. 1984) (citations omitted)) (defining horizontal commonality).

105 Elzweig & Trautman, *supra* note 35.

106 Sabrina Ortega, *NFTs and fNFTs – Priceless Collectables, Digital Trinkets, or Regulatable Securities?*, U. MIA. BUS. L. REV. INSIGHTS (Jan. 21, 2022), https://business-law-review.law.miami.edu/nfts-and-fnfts-priceless-collectables-digital-trinkets-or-regulatable-securities/.

107 *Id.*

108 Miriam R. Albert, *The* Howey *Test Turns 64: Are the Courts Grading This Test on a Curve?*, 2 WM. & MARY BUS. L. REV. 1, 23 (2011).

109 Elzweig & Trautman, *supra* note 35.

110 *Id.*

For an NFT to be considered a security, in addition to commonality, the third and fourth prongs of the *Howey* Test must be met.[111] The third and fourth prongs of *Howey* require there be an expectation of profits and that the profits must come from the essential entrepreneurial efforts of others.[112] These prongs would also be looked at on a case-by-case basis.[113] Traditional NFTs do not usually have the expectation of profits from the entrepreneurial efforts of others. Traditional NFTs are usually bought as a commodity, and although they may rise or fall in value, they usually do so due to market fluctuations, not because of the entrepreneurial efforts of others.[114] The *Framework* states that "[p]rice appreciation resulting *solely* from external market forces (such as general inflationary trends or the economy) impacting the supply and demand for an underlying asset generally is not considered 'profit' under the Howey test."[115] Once an NFT is fractionalized, there likely becomes an expectation of profits - especially if the shards are marketed as an investment. Oftentimes when shards are issued, the issuer retains a degree of managerial control of the underlying asset that the F-NFT represents.[116] The shards then may be sold on secondary markets, where they increase in value. If the profit is derived from the seller's efforts and the seller has retained control of a portion of the underlying asset, the last two prongs of the *Howey* Test would be met.[117] While it is unlikely that traditional NFTs would be considered a security, F-NFTs in most cases would be.[118]

D. Impact of FTX Failure

In November 2022, reports emerged that, in just a few days, cryptocurrency billionaire Samuel Bankman-Fried witnessed his $32 billion company plunge into bankruptcy and he became the target of DOJ and SEC investigations.[119] Trautman has written that "[t]he demise of FTX and its many related crypto entities created contagion and collateral damage for other participants and investors in the cryptocurrency community."[120] In addition, "[t]he U.S. bankruptcy proceedings of many FTX related entities, scattered across many jurisdictions worldwide, will

---

111 Goforth, *supra* note 33, at 649.

112 *Id.*

113 Bull & Harttraft, *supra* note 66, at 14.

114 Elzweig & Trautman, *supra* note 35.

115 FRAMEWORK, *supra* note 69, at 4–5.

116 Arben Kane, *Fractionalized NFT (F-NFTs): All That You Need to Know*, MEDIUM (Sept. 9, 2021), https://medium.com/@arbenk/fractionalized-nft-f-nfts-all-that-you-need-to-know-46bc06ea486d.

117 Elzweig & Trautman, *supra* note 35.

118 *Id.*

119 Lawrence J. Trautman, *The FTX Crypto Debacle: Largest Fraud Since Madoff?* (Dec. 24, 2022) (unpublished manuscript), http://ssrn.com/abstract=4290093.

120 *Id.* at 1.

likely take years to sort out."[121] Early reports indicate that FTX owes an estimated $8 billion to its creditors (including customers), numbering in the hundreds of thousands. Due to the negative impact on so many individuals worldwide, it is now probable that the demise of FTX will result in significant legislation and legal remedies impacting the topic of this Article.

E. Commodity Futures Trading Commission, Federal Reserve, and Other Regulators

In recent years, the dramatic growth of cryptocurrencies has attracted the close attention of Congress, the U.S. Federal Reserve System, the U.S. national security infrastructure, law enforcement authorities, the SEC, the Commodity Futures Trading Commission (CFTC), and others.[122]

V. QUANTUM COMPUTING

Growing recognition of the future significance of quantum computing is evidenced by the awarding of the 2022 Nobel Prize in Physics to John Clauser of Walnut Creek, California; Alain Aspect of France; and Anton Zeilinger of the University of Vienna in Austria.[123] Upon announcement of these awards, *The New York Times* reports: "Their independent works explored the foundations of quantum mechanics, the paradoxical rules that govern behavior in the subatomic world. In experiments conducted over the last 50 years, they confirmed the reality of an effect that Albert Einstein had distained as 'spooky action at a distance.'"[124] It appears that "[m]easuring one of a widely separated pair of particles could instantaneously change the results of measuring the other particles, even if it was light years away. Today, physicists call this strange effect quantum entanglement and it is the basis of the burgeoning field of quantum information."[125]

A. How and Why Important

The potential application of quantum mechanics to business and societal problems (particularly climate) is significant.[126] While the future impact of advances in quantum mechanics cannot now be fully understood, "[q]uantum

---

121 *Id.*

122 *Id.*

123 Isabella Kwai, Cora Engelbrecht & Dennis Overbye, *3 Who Opened Field of Quantum Entanglement, and Undermined Einstein*, N.Y. TIMES, Oct. 5, 2022, at A9.

124 *Id.*

125 *Id.*

126 Lawrence J. Trautman & Neal Newman, *The Environmental, Social and Governance (ESG) Debate Emerges from the Soil of Climate Denial*, 53 U. MEMPHIS L. REV. (forthcoming), http://ssrn.com/abstract=3939898.

computing promises to solve complex problems that existing supercomputers are unable to handle, such as understanding patterns in the folding of human proteins to discover new drugs, climate change, or maximizing shipping routes for several hundred tankers."[127] Of major importance, "[e]xisting quantum computers are smaller and require less energy than supercomputers. An IBM quantum processor chip is slightly larger than ones found in laptops."[128] Followers of blockchain-related technologies will immediately recognize that improvement upon blockchain's unfavorable energy-consumption issue is of major impact. Journalist Karen Hao writes:

> Quantum computers derive their extraordinary speed from their use of so-called quantum bits, or qubits, instead of the digital zeros and ones used to represent data in conventional computers.
> Bits, as those zeros and ones are known, can only have a single value. But qubits—which are encoded into subatomic and atomic particles including electrons, photons and ions—can exist as a zero and a one at the same time. This phenomenon, known as superposition, makes qubits superbly efficient at handling certain calculations, such as those required to simulate the physical world or optimize business processes.[129]

Several recent federal developments point to recognition of the significant importance of quantum computing to future technological advances and national security: Executive Order 14028; National Security Memorandum 8 (NSM-8); and National Security Memorandum 10 (NSM-10). Each of these developments will now be discussed.

B. Executive Order 14028

Issued on May 12, 2021, President Biden's Executive Order 14028 recognizes that "[t]he United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors."[130] EO 14028 states:

> The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons

---

127 Benjamin Katz & Eric Niiler, *Nobel Awarded for Quantum Computing,* WALL ST. J., Oct. 5, 2022, at A3.
128 *Id.*
129 Karen Hao, *China Leaps Into Quantum Computing Race*, WALL ST. J., Oct. 7, 2022, at B1.
130 Exec. Order No. 14028, 86 Fed. Reg. 26633, 26633 (May 17, 2021).

> learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced. Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).[131]

The Biden Administration states: "the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth . . . ."[132] EO 14028 directed multiple federal agencies to "enhance[e] cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain."[133] The National Institute of Standards and Technology (NIST) reports that:

> Section 4 directs NIST to solicit input from the private sector, academia, government agencies, and others and to identify existing or develop new standards, tools, best practices, and other guidelines to enhance software supply chain security. Those guidelines, **which are ultimately aimed at federal agencies but which also are available for industry and others to use**, include:
> criteria to evaluate software security,
> criteria to evaluate the security practices of the developers and suppliers, and

---

131 *Id.*
132 *Id.*
133 *Id.*

> innovative tools or methods to demonstrate conformance with secure practices.[134]

C. NSM-8

It is NSM-8 that implements the EO 14028 cybersecurity requirements "for National Security Systems (NSS) – networks across the U.S. Government that contains classified information or are otherwise critical to military and intelligence activities."[135] NSM-8

> provides the National Manager the authority to issue binding direction to departments and agencies operating NSS to take action against cybersecurity threats and vulnerabilities. All departments and agencies operating NSS will now report to the National Manager on both the status of mitigation actions taken in response to a specific cyber incident as well as provide assessments of the overall impact to their systems. Departments and agencies are also required to notify the National Manager of known or suspected incidents or compromises of NSS.[136]

Modernized encryption protocols are also required of federal departments and agencies in use for national security systems.[137] General Paul M. Nakasone, Commander of U.S. Cyber Command, Director of the NSA and Chief of the Central Security Service states, "As the nation's leader in cryptography, NSA will play a significant role in ensuring cryptographic interoperability among national security system users through cryptographic standards for use on NSS."[138]

D. NSM-10

Of most impact to the authors' inquiry is NSM-10, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems"[139] NSM-10 "seeks

---

134 *Executive Order 14028, Improving the Nation's Security*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity (last visited Dec. 24, 2022).

135 *President Biden Signs Cybersecurity National Security Memorandum*, NAT'L SEC. AGENCY (Jan. 19, 2022), https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2904637/president-biden-signs-cybersecurity-national-security-memorandum/.

136 *Id.*

137 *Id.*

138 *Id.*

139 Joseph R. Biden Jr., *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, THE WHITE HOUSE (May 4, 2020), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04

to promote U.S. leadership in quantum information science (QIS) . . . [and] also addresses potential threats that quantum computers may pose to encrypted data and systems."[140] The risk noted by the Congressional Research Service that "[a] mathematician has already developed the algorithm to break today's encryption with quantum computers"[141] is significant to the focus here about the potential for quantum computing to successfully hack current encryption technology, and perhaps blockchain.

D. Impact on Cryptography

For the purposes of this Article, the authors are particularly interested in the likely impact of quantum mechanics technology on the potential for future cybersecurity and associated risk. *The New York Times* reported that recently:

> [A]s scientists have done more experiments with entangled particles, entanglement has become accepted as one of main features of quantum mechanics and is being put to work in cryptology, quantum computing and an upcoming 'quantum internet' to the tune of more than a billion dollars a year. One of its first successes in cryptography is messages sent using entangled pairs, which can send cryptographic keys in a secure manner—any eavesdropping will destroy the entanglement, alerting the receiver that something is wrong.
>
> In 2017, Dr. Zeilinger used this technique with entangled photons beamed from a Chinese satellite called Micius to have an encrypted 75-minute video conversation with Jian-Wei Pan of the Chinese Academy of Sciences, one of his former students.[142]

Quantum computing is an emerging technology that, while providing immense capability to solve problems that today's computers cannot, will also pose a risk to the foundation of numerous blockchain technologies. IBM's Public Sector Lead for Quantum Computer, Critical Infrastructure Protection, and Innovation described quantum computing in front of the House Subcommittee on Cybersecurity as follows:

/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

[140] CONG. RSCH. SERV., PREPARING SECRETS FOR A POST-QUANTUM WORLD —NATIONAL SECURITY MEMORANDUM 10, IN11921 at 1 (2022), https://crsreports.congress.gov/product/pdf/IN/IN11921.

[141] *Id.* at 2.

[142] Isabella Kwai, Cora Engelbrecht & Dennis Overbye, *3 Who Opened Field of Quantum Entanglement, and Undermined Einstein,* N.Y. TIMES, Oct. 5, 2022, at A9.

> Quantum computing is not simply a faster way of doing what today's computers do – it is a fundamentally different approach that promises to solve problems that classical computing cannot realistically solve. Quantum computers are not simply more powerful supercomputers. Instead of computing with the traditional bit of a 1 or 0, quantum computers use quantum bits, or qubits (CUE-bits), that can run multidimensional quantum algorithms. Think of it this way, a classical supercomputer solves a problem sequentially. Supercomputers leverage their many processors to explore every possible path to a solution before arriving at an answer. But as the problem and data grow more complex, there simply isn't enough computing power to solve problems that grow exponentially. For example, there are 40 thousand different ways to seat 8 people around a table. If you add one person, it becomes 362 thousand. Make it 10 people and the number of combinations is more than 3.5 million. Eleven people, almost 40 million. No existing computer has the working memory to handle all the possible combinations as problem sizes grow exponentially large. By contrast, a quantum computer can double the size of the problem space it can analyze by adding only one qubit.[143]

While it is known that quantum computers will provide these immense capabilities, it is not known when enough technological advances will be made that a quantum computer with enough computational power that is capable of error correction to begin tackling existing problems will be available. Still, many experts predict it will be within the decade.[144]

E. The Impact of Quantum Computing on Blockchain

Quantum computing challenges a key aspect of blockchain: cryptography. Today's cryptographic protocols, which underpin blockchain technology, are based on mathematical problems that a traditional computer cannot easily solve. This is typically the factoring of large numbers—for example, when given a number (encrypted data), finding which two numbers are multiplied together to give the original number. The power in this technique is that finding these factors

---

[143] *Securing the Future: Harnessing the Potential of Emerging Technologies While Mitigating Security Risks Before the H. Subcomm. on Cybersecurity, Infrastructure Protection, & Innovation of the H. Comm. on Homeland Sec.*, 117th Cong. (2022) (statement of Charles W. Robinson, Public Sector Leader, Quantum Computing, IBM), https://homeland.house.gov/imo/media/doc/robinson_testimony_cipi_062222.pdf.

[144] *Id.*

is hard but easy to check. Standard computers can test thousands of options in an attempt to find a solution, but as the numbers grow bigger, this becomes exponentially harder and out of the limits of achievable computational power. However, quantum computers work differently and can leverage an algorithm (Shor's algorithm), which enables a quantum computer to use its unique computing power to find these prime factors in significantly less time.[145] As quantum computers become robust enough to leverage Shor's algorithm, the underlying cryptographic algorithm breaks, and the information is no longer secure. Thus, the arms race continues—the world, as it has with past encryption techniques dating back millennia to a simple Caesar cipher in which each letter was shifted along the alphabet by a set number, will need to adopt new methods of encrypting and securing information.

F. Securing the Future of Crypto

Before adopting new techniques, the algorithms must first be developed, tested, and standardized. In 2016, the NIST announced a competition to identify algorithms that would be resistant to the attacks of quantum computing and Shor's algorithm, called post-quantum cryptographic algorithms. This work of developing standards has undergone years of competition involving government, industry, and academic institutions from around the world, working across four rounds of exploration, submissions, and testing.[146] The culmination of this work resulted in an announcement by the NIST, in 2022, of the selection of four initial algorithms for standardization.[147] These algorithms will undergo a process in which discrete standards will be developed and published for organizations to adopt through implementation sometime between 2022 and 2024.[148] These standards will enable the cryptographic community to begin to build tools and adopt into existing products such that computer systems will continue to be interoperable.

G. The Transition

The adoption of these algorithms will not happen overnight. As the community has seen with past upgrades and transitions of cryptographic

---

[145] Jennifer Chu, *The Beginning of the End for Encryption Schemes?*, MASS. INST. OF TECH.: MIT NEWS (Mar. 3, 2016), https://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303.

[146] Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms, 81 Fed. Reg. 92787 (Dec. 20, 2016).

[147] *Selected Algorithms*, NAT'L INST. OF STANDARDS & TECH.: POST-QUANTUM CRYPTOGRAPHY (Nov. 29, 2022), https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[148] *Workshops and Timeline*, NAT'L INST. OF STANDARDS & TECH.: POST-QUANTUM CRYPTOGRAPHY (Nov. 29, 2022), https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline.

algorithms, it can take a long time. For instance, SHA1, an old cryptographic algorithm, was deprecated by the NIST over a decade ago yet is still used today by organizations.[149] This is despite SHA2, the successor to SHA1, being available as far back as 2006.[150]

While the standards for these new post-quantum cryptographic algorithms are not yet available, organizations must act now to more quickly incorporate these updates into their systems and crucially allow for the algorithms that underly blockchain to be updated. As detailed, these algorithms underpin blockchain technology and the way that access to these systems typically works is through digital keys. Organizations can begin acting now for these coming transitions by preparing things like budgets, policy updates, inventories of existing systems, and plans for testing.

VI. NATIONAL SECURITY IMPLICATIONS

By now, many years of credible warnings document the use of cyber exploits by nation- states as weapons against others.[151] President Biden's National Security Strategy observes that "[t]echnology is central to today's geopolitical competition and to the future of our national security, economy and democracy. U.S. and allied leadership in technology and innovation has long underpinned our economic prosperity and military strength."[152] Regarding the securing of cyberspace, The U.S. National Security Strategy states:

> Our societies, and the critical infrastructure that supports them, from power to pipelines, is increasingly digital and vulnerable to disruption or destruction via cyber- attacks. Such attacks have been used by countries, such as Russia, to undermine countries' ability to deliver services to citizens and coerce populations. We are working closely with allies and partners, such as the Quad, to

---

[149] *NIST Policy on Hash Functions*, NAT'L INST. OF STANDARDS & TECH.: HASH FUNCTIONS (Nov. 29, 2022), https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions; Pavel Raiskup, *Enhancing RHEL Security: Understanding SHA-1 Deception on RHEL 9*, RED HAT: RED HAT BLOG (July 25, 2022), https://www.redhat.com/en/blog/rhel-security-sha-1-package-signatures-distrusted-rhel-9.

[150] *Id.*

[151] *See, e.g.*, Lawrence J. Trautman, *Is Cyberattack the Next Pearl Harbor?,* 18 N.C. J. L. & TECH. 233 (2016), http://ssrn.com/abstract=2711059; Lawrence J. Trautman, *Impeachment, Donald Trump and The Attempted Extortion of Ukraine*, 40 PACE L. REV. 141 (2020), http://ssrn.com/abstract=3518082; Lawrence J. Trautman, Tik Tok! TikTok: Escalating Tension Between U.S. Privacy Rights and National Security Vulnerabilities (Feb. 13, 2023) (unpublished manuscript) (SSRN), http://ssrn.com/abstract=4163203.

[152] OFF OF THE PRESIDENT, NATIONAL SECURITY STRATEGY 32 (2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

> define standards for critical infrastructure to rapidly improve our cyber resilience, and building collective capabilities to rapidly respond to attacks. In the face of disruptive cyber attacks from criminals, we have launched innovative partnerships, to expand law enforcement cooperation, deny sanctuary to cyber criminals and counter illicit use of cryptocurrency to launder the proceeds of cybercrime. As an open society, the United States has a clear interest in strengthening norms that mitigate cyber threats and enhance stability in cyberspace. We aim to deter cyber attacks from state and non state actors and will respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure. We will continue to promote adherence to the UN General Assembly-endorsed framework of responsible state behavior in cyberspace, which recognizes that international law applies online, just as it does offline.[153]

Recent reports show that "[a] growing body of evidence suggest that pro-Russian hackers and online activists are working with the country's military intelligence agency, according to researchers at Google."[154] *The Wall Street Journal* reports:

> Western officials and security experts are interested in the possible Kremlin links because it would help explain Moscow's intentions both inside and outside Ukraine despite recent military setbacks that prompted Russian President Vladimir Putin this week to announce a mobilization push.
>
> Officials in the U.S. and Europe have warned throughout the war that Russian hackers could lash out against Ukraine's allies by targeting critical infrastructure and governments with cyberattacks, but so far that has largely failed to materialize.
>
> Over the past few months, Google's Mandiant cybersecurity group has observed apparent coordination between pro-Russian hacking groups—ostensibly comprising patriotic citizen hackers—and cyber break-ins by Russia's military intelligence agency, or GRU. In four instances, Mandiant says it observed hacking activity linked

---

[153] *Id.* at 34.

[154] Robert McMillan & Dustin Volz, *Google Sees Russia Coordinating With Hackers in Cyberattacks Tied to Ukraine War,* WALL ST. J. (Sept. 26, 2022), https://www.wsk.com/articles/google-sees-russia-coordinating-with-hackers-in-cyberattacks-tied-to-ukraine-war-11663930801.

> to the GRU in which malicious "wiper" software was installed on a victim's network.[155]

In October 2022, the chief of United Kingdom's electronic intelligence agency warned, "Beijing's efforts to exert control over technology both internationally and within China's boarders threaten future global security and freedom."[156] Jeremy Fleming, director of United Kingdom's Government Communications Headquarters contends that "Beijing was aiming to use an array of existing and emerging technological means, including digital currency and satellites, to control markets and people, extend surveillance and censorship and export its authoritarian system around the world."[157] This warning includes "China's expanding use of technology to control dissent and its growing ability to attack satellite systems, control digital currencies and track individuals pose far deeper challenges for the West."[158]

A. Systemic Threats Posed by Rapid Technological Change

On October 3, 2022, the Financial Stability Oversight Council (the "Council") released its *Report on Digital Asset Financial Stability Risks and Regulation*.[159] The report warns that "[c]rypto-asset activities could pose risks to the stability of the U.S. financial system if their interconnections with the traditional financial system or their overall scale were to grow without adherence to or being paired with appropriate regulation, including enforcement of the existing regulatory structure."[160] The Council observed:

> The scale of crypto-asset activities has increased significantly in recent years. Although interconnections with the traditional financial system are currently relatively limited, they could potentially increase rapidly. Participants in the crypto-asset ecosystem and the traditional financial system have explored or created a variety of interconnections. Notable sources of potential

---

155 *Id.*

156 Dustin Volz, Chinese Tech Threatens Future Global Security, U.K. Spy Chief Warns, WALL ST. J. (Oct. 11, 2022), https://www.wsj.com/articles/chinese-tech-threatens-future-global-security-warns-u-k-spy-chief-11665502252.

157 *Id.*

158 David E. Sanger, *British Intelligence Official Focuses on China Threat,* N.Y. TIMES, Oct. 11, 2022, at A8.

159 FIN. STABILITY OVERSIGHT COUNCIL, REPORT ON DIGITAL ASSET FINANCIAL STABILITY RISKS AND REGULATION (2022), https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf.

160 *Fact Sheet: The Financial Stability Oversight Council's Report on Digital Asset Financial Stability Risks and Regulation*, U.S. DEP'T OF TREASURY (Oct. 3, 2022), https:home.treasure.gov/system/files/261/Fact-Sheet-Report-on-Digital-Asset-Financial-Stability-Risks-and-Regulation.pdf.

> interconnections include traditional assets held as part of stablecoin activities. Cryptoasset trading platforms may also have the potential for greater interconnections by providing a wide variety of services, including leveraged trading and asset custody, to a range of retail investors and traditional financial institutions. Consumers can also increasingly access cryptoasset activities, including through certain traditional money services businesses.
> Some characteristics of crypto-asset activities have acutely amplified instability within the crypto-asset ecosystem.
> • Many crypto-asset activities lack basic risk controls to protect against run risk or to help ensure that leverage is not excessive.
> • Crypto-asset prices appear to be primarily driven by speculation rather than grounded in current fundamental economic use cases, and prices have repeatedly recorded significant and broad declines.
> • Many crypto-asset firms or activities have sizable interconnections with crypto-asset entities that have risky business profiles and opaque capital and liquidity positions.
> • In addition, despite the distributed nature of crypto-asset systems, operational risks may arise from the concentration of key services or from vulnerabilities related to distributed ledger technology.[161]

On October 7, 2022, *The Wall Street Journal,* in an observation having profound national security implications, reported that "China is making new strides in its bid to join the U.S. as a leader in quantum computing, a promising but elusive technology that could one day supercharge scientific research and transform data-intensive industries ranging from finance and pharmaceuticals to logistics and green energy."[162] Advances in these new technologies may determine global, political, and economic stability in the future.

VII. INJURY AND LEGAL RECOURSE

Currently no criminal or civil statutes explicitly punish a 51% attack. This section examines the strengths and weaknesses of different causes of action for prosecuting such an attack. The different causes of action include SEC and CFTC enforcement, larceny and wrongful appropriation statutes, the Computer Fraud and Abuse Act, fraud statutes, antitrust statutes, and wire fraud statutes. Furthermore, this section analyzes the potential defense of consent and assumption of risk.

---

[161] *Id.*; *see also* Mengqi Sun, *Treasury Aims at Illicit Crypto Risks,* WALL ST. J., Sept. 20, 2022, at B10.

[162] Hao, *supra* note 132, at B1.

A. 51% (Goldfinger) Attack Defined

Professor Joseph Bonneau reports that it was "known from the start that an attacker with a majority of computational power [51%] can easily cause arbitrary deep forks in the blockchain."[163] Scholarship in recent years has "shown that an attacker with substantially less power can, at the very least, undermine the fair distribution of rewards in the system."[164] Such an attacker who would seek to undermine the "stability of consensus protocols were described by Kroll et al. as a Goldfinger attacker after the James Bond villain who attempted to irradiate US Treasury reserves."[165] Given the likelihood of a 51% (Goldfinger) attack, addressing the issue of potential legal recourse is as timely as it is pressing and consequential.[166]

B. SEC Enforcement

As previously discussed, there is widespread disagreement as to whether cryptocurrencies are securities for purposes of SEC regulation.[167] The two main cryptocurrencies, Bitcoin and Ether, likely are not.[168] If a 51% attack occuresoccurs on a cryptocurrency that is considered a security and regulated by the SEC, the action risks potential liability from the SEC. However, the unique nature of cryptocurrencies and a 51% attack mean that the applicability of existing SEC regulations is unclear.

15 U.S.C. § 78i, which prohibits manipulation of security prices, is one statute that could potentially be used to prosecute a 51% attack. "[I]t shall be unlawful for any person, directly or indirectly by the use of the mails or any means or instrumentality of interstate commerce . . . . for the purpose of creating a false or misleading appearance . . . with respect to the market for any such security."[169] However, the statute explicitly applies only to a purchase, sale, or securities swap conducted to manipulate the price. Even § 78i(a)(4), which covers manipulating the market with false or misleading statements, is explicitly limited to the buying and selling of securities. While a 51% attack does manipulate the price of the

---

[163] Joseph Bonneau, *Hostile Blockchain Takeovers*, FINANCIAL CRYPTOGRAPHY AND DATA SECURITY - FC 2018 INTERNATIONAL WORKSHOPS, BITCOIN, VOTING, AND WTSC, REVISED SELECTED PAPERS 92 (Jeremy Clark, Massimiliano Sala, Ittay Eyal, Vanessa Teague, Andrea Bracciali, Aviv Zohar & Federico Pintore ed., 2019).

[164] *Id.*

[165] *Id.* (citing J.A. Kroll, I.C. Davey & E.W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries,* TWELFTH WORKSHOP ON THE ECONS. INFO. SEC (2013), https://asset-pdf.scinapse.io/prod/2188530018/2188530018.pdf)).

[166] *Cost of a 51% Attack*, GOBITCOIN.IO https://gobitcoin.io/tools/cost-51-attack/ (last visited Oct. 22, 2022).

[167] *See supra* 99-122 and accompanying text.

[168] *Id.*

[169] 15 U.S.C. § 78i(a).

cryptocurrency, it is not performed by buying, selling, or swapping the asset, as required under 18 U.S.C. § 78i.

The SEC is certainly aware of 51% attacks but has not passed any guidance on the criminality of such an occurrence.[170] The lack of guidance by the SEC supports the position that existing regulations do not provide the opportunity for prosecution against a 51% attack. However, language used by the SEC when discussing a 51% attack may shed light on potential criminal liability. The SEC has described a 51% attack as: when "a bad actor that controls a majority of the processing power dedicated to mining on the bitcoin network may be able to alter the bitcoin blockchain on which the bitcoin network and bitcoin transactions rely."[171] Referring to the perpetrator of a 51% attack as a "bad actor" implies that the SEC does not believe that a 51% attack is a feature of the blockchain and all who hold a cryptocurrency are consenting to such an occurrence. The term "bad actor" further implies that a criminal mens rea is present.

C. CFTC Enforcement

The CFTC has asserted their authority to regulate cybercurrencies as commodities under the Commodities Exchange Act (CEA).[172] The CFTC's Division of Enforcement has brought a commodities fraud action against Samuel Bankman-Fried and FTX regarding the sale of crypto assets that led to the FTX failure.[173] However, CFTC commodities fraud actions would likely be ineffective against a 51% attack. The CFTC posture regarding 51% attacks is similar to that of the SEC. Although the CFTC is aware of 51 % attacks, it has not passed any guidance regrading enforcement of those attacks. CEA section 6(c)(1)[174] and CFTC Regulation 180.1(a),[175] the broad fraud provisions of the CEA, only apply to transactions in connection with swaps, contracts of sale, or future sale of commodities. While it may be argued that a 51% attack is an artifice to defraud, it would not be a transaction connected to a swap or commodity sale, leaving it outside of the jurisdiction of prosecution by the CFTC.

---

170 *See, e.g.*, Self-Regulatory Organizations; Bats BZX Exchange, Inc.; Order Setting Aside Action by Delegated Authority and Disapproving a Proposed Rule Change, as Modified by Amendments No. 1 and 2, to List and Trade Shares of The Winklevoss Bitcoin Trust, Exchange Act Release No. 93559 (July 26, 2018), 2018 WL 11274418.

171 *Id.*

172 *Digital Assets*, CFTC, https://www.cftc.gov/digitalassets/index.htm (last visited Jan. 4, 2023).

173 Complaint, CFTC v. Samuel Bankman-Fried, FTX Trading Ltd D/B/A FTX.com, & Alameda Research LLC, No. 1:22-CV-10503 (S.D. N.Y. Dec. 13, 2022).

174 7 U.S.C. § 6(c)(1).

175 17 C.F.R. § 180.1.

D. Larceny and Wrongful Appropriation

If the perpetrator of a 51% attack was a member of the armed forces,10 U.S.C. § 921, the larceny and wrongful appropriation provision in the Military Code of Justice, could potentially be applied. This statute states: Any person subject to this chapter who wrongfully takes, obtains, or withholds, by any means, from the possession of the owner or of any other person any . . . personal property . . . with intent permanently to deprive or defraud another person of the use and benefit of the property or to appropriate it to his own use or the use of any person other than the owner, steals that property and is guilty of larceny.

While cryptocurrencies likely constitute personal property,[176] and the victims of a 51% attack have had their personal property permanently deprived, it is still unclear if a 51% attack would be in violation of this statute. Even in considering the intangible ones and zeros of the code, the perpetrators of the 51% attack technically did not deprive anyone of ownership in that. First, the code is publicly available and not owned by any one person. Second, and relatedly, the attackers did not deprive anyone of that code. They simply created alternative code that became more popular.

A more common version of cryptocurrency theft in which a hacker sells off a victim's cryptocurrency after acquiring access to the victim's wallet key, a trade secrets theory could be argued. Here, it is not the deprivation of cryptocurrency that is the main issue; rather, it is the taking of a trade secret (the wallet key).

E. Computer Fraud and Abuse Act

At least one commentator has proposed that the Computer Fraud and Abuse Act (CFAA) could potentially be used to prosecute the perpetrators of a 51% attack.[177] The statute punishes anyone who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[178] The following is an examination of four of the necessary elements:

1. "Knowingly"

It is possible for a cryptocurrency miner to inadvertently transmit information to the blockchain network. However, this is not the case in a 51%

---

[176] This has yet to be adjudicated in America. The British legal system, while not dispositively, has strongly indicated that cryptocurrencies are property. A. Taylor & M. Ó Floinn, *Bitcoin Burglaries and the Theft Act 1968*, (3) CRIM. L. REV. 163 (2021).

[177] Kiara Taylor, *What Happens in 51% Attacks?*, ALEXANDRIA, https://coinmarketcap.com/alexandria/article/what-happens-in-51-attacks (last visited Dec. 15, 2022).

[178] 18 U.S.C. § 1030(a)(5)(A).

attack. A cryptocurrency miner engaged in a 51% attack would be conducting actions such as confirming transactions that did not occur, refusing to confirm legitimate transactions, or otherwise reorganizing transactions. These are not actions that can be performed unintentionally.

2. "Cause Damage"

The term "damage" is defined in the statute as "any impairment to the integrity or availability of data, a program, a system, or information."[179] A 51% attack certainly alters blockchain data but it is unclear if such an action could be said to impair the integrity of the data. The victims of a 51% attack would likely maintain that the integrity of the blockchain has been impaired. But this colloquial interpretation may not be consistent with the statutory intent from 1984, which was drafted long before the blockchain and 51% attacks were conceived.

It would likely be easier for a prosecutor to satisfy this damage requirement by focusing on the "availability of data" aspect. A 51% attack is likely to involve taking some previously available data and deleting it from the blockchain, thus impairing the availability of the data. However, this is only true in a limited sense. The data would still be "available" in that there would still exist some record of it. But, the data would just no longer be available as a functioning part of the blockchain.

The statute's definition of what constitutes a "loss" is somewhat inconsistent with its applicability to a 51% attack. "Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[180] This definition was clearly written with a more traditional computer hacking attack in mind. The "loss" incurred from a 51% attack would likely not include costs related to responding to the offense, restoring data, lost revenue, or interrupted service.

3. "Without Authorization"

This element is ambiguous as to whether it refers only to transmitting data to another computer "without authorization"[181] or if it refers more broadly to the

---

179 18 U.S.C. § 1030(e)(8).

180 18 U.S.C. § 1030(e)(11).

181 *See, e.g.*, Advanced Aerofoil Techs., AG v. Todaro, No. 11 Civ. 9505(ALC)(DCF), 2013 WL 410873, at *8 (S.D.N.Y. Jan. 30, 2013).

"damage" to a protected computer occurring "without authorization."[182] The Nebraska federal district court has explained the majority rule that "without authorization" modifies "intentionally causes damage" and not accessing the computer.[183] Under this majority interpretation, the victims of a 51% attack could allege that, while the 51% attackers did have authorization to the code they manipulated, it is the harm to the victims that they were lacking in authorization.

This second, majority interpretation further helps a potential victim of a 51% attack because it is more likely to cover the deleting of information that leads to damage and not just the transmission of data. Even with the first, more defendant-friendly interpretation of "without authorization," the victims could argue that, while the attackers did have authorized access to the blockchain, they clearly exceeded this authorized access when they maliciously manipulated the code against the clearly established principles for personal gain.

Again, this statute was written to addresswith more traditional computer hacking situation and not a 51% cryptocurrency attack. A minority victim of such an attack could allege that he or she did not "authorize" the attack. But the 51% attackers did not gain unauthorized access to anything. They were operating within the parameters of the network as designed. Here, open world video games can be used as a helpful analogy. When other players on the network decide to forcefully take another player's property and/or life, the victim could allege that he or she did not "authorize" the attack. But the attackers were, in a sense, authorized to perform such actions by the game's code which allows for such an occurrence. Much like the victim in the video game analogy, it could be argued that minority victims of a 51% attack implicitly "authorized" such an attack by participating in a blockchain program in which such attacks are possible.

For example, elsewhere in the statute, the term "exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."[184] But this is not the kind of authorization at issue in a 51% attack because the users causing the 51% attack do have authorization to the blockchain.

4. "To a Protected Computer"

The term "protected computer" is defined broadly by the statute as "a computer . . . which is used in or affecting interstate or foreign commerce or communication . . . ."[185] Therefore, this element of the statute appears to be clearly met.

---

[182] *See, e.g.*, U.S. v. Stratman, No. 4:13-CR-3075, 2013 U.S. Dist. LEXIS 150224, at *3–7 (D. Neb. Aug. 5, 2013).

[183] *Id.* at *5.

[184] 18 U.S.C. § 1030(e)(6).

[185] § 1030(e)(2)(B).

5. Civil and Criminal Punishments under the CFAA

The CFAA provides for both criminal and civil punishments. Someone found guilty of violating the relevant section discussed here could face a fine and up to ten years imprisonment or twenty years for a repeat offense.[186] These are the same punishments for someone convicted of attempting to violate the CFAA.[187] Any victim of a CFAA violation who suffers more than $5,000 in damages has civil recourse as provided under the statute.[188]

F. Fraud

Prosecution under a fraud statute is another potential cause of action. However, fraud statutes likely do not apply to cryptocurrency majority attacks. 18 U.S.C. § 1341 Frauds and Swindles states:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do . . . . such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.[189]

The definition of "scheme or artifice to defraud" includes "a scheme or artifice to deprive another of the intangible right to honest services."[190] Since Bitcoin is used to purchase goods and services, it could be argued that a 51% attack that deletes the Bitcoins of vendors who accepted them in exchange for honest services may meet this definition.

This statute also forbids "obtaining money or property by means of false or fraudulent pretenses, representations, or promises . . . ."[191] Depending on whether a particular cryptocurrency is defined as "money" or not and how the 51% attack

---

186 § 1030(c)(4)(B), (C).
187 § 1030(c)(4)(B)(ii), (C)(ii).
188 § 1030(g).
189 § 1341.
190 § 1346.
191 § 1341.

is performed,[192] it could be argued that the perpetrators of the attack have "obtained money" from the victims.

Another federal fraud statute that could potentially be applied to the perpetrators of a 51% attack is 18 U.S.C. § 1029 (fraud and related activity in connection with access devices):

> Whoever . . . knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000 . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.[193]

The term "access device" is defined broadly as:

> any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).[194]

However, a 51% attack would likely not be interpreted to involve gaining access to the device of another, as the necessary alterations to the blockchain can be performed without doing so.

G. Antitrust Legislation

Antitrust legislation provides another potential cause of action against the perpetrators of a 51% attack. 15 U.S.C. § 1 states:

> Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal. Every

---

[192] For example, did the 51% attack erase the victims' coins from the blockchain (in which case, the victims were deprived of those coins but the perpetrators of the attack did not literally "obtain" those coins)? Or did the 51% attack convert the victims' coins to the attackers' possession (in which case they did "obtain" the coins from the victims)? Furthermore, since the ultimate outcome of these two methods would be similar (deleting 49% of the coins from the blockchain would result in increasing the value of each remaining coin), would courts treat them the same?

[193] 18 U.S.C. § 1029(a)(5).

[194] § 1029(e)(1).

> person who shall make any contract or engage in any combination or conspiracy hereby declared to be illegal shall be deemed guilty of a felony, and, on conviction thereof, shall be punished by fine not exceeding $100,000,000 if a corporation, or, if any other person, $1,000,000, or by imprisonment not exceeding 10 years, or by both said punishments, in the discretion of the court.[195]

In situations whereno one person maintains 51% of the mining power for a cryptocurrency, a 51% attack would require collusion between two or more people. This collusion would result in excluding the victims from participating in that particular cryptocurrency market. However, this exclusion would only be temporary, as the victims could simply purchase the cryptocurrency—although at the newly inflated cost—and be back in that market.

H. Wire Fraud

18 U.S.C. § 1343 states:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.[196]

This wire fraud statute could provide a cause of action against a 51% attack, assuming cryptocurrencies are defined as property.[197] The perpetrators of the attack could be said to have devised a scheme to obtain the property of others through fraudulent pretenses. Much like the previously discussed fraud statutes, a successful prosecution may hinge on whether the victimized holders of the cryptocurrency are determined to have assumed the risk of such an attack and therefore implicitly consented to such an outcome. If the victims are seen as assuming the risk, then it would not be the case that they were deprived of their cryptocurrency by fraud; rather, they simply received an unfortunate outcome, which was a risk they knowingly undertook.

---

195 15 U.S.C. § 1.

196 18 U.S.C. § 1343.

197 *See*, *supra* note .

I. Consent / Assumption of Risk

A problem with criminal and civil liability for a 51% attack is the ambiguity surrounding how cryptocurrencies are owned. For example, is cryptocurrency ownership based on possession of the private key or based on the blockchain consensus? If cryptocurrency ownership is determined to be contingent upon the consensus of the blockchain, then a strong argument could be made that owners implicitly consent to blockchain alterations, even ones that result in the loss of their coins.

Consensus mechanisms, such as cryptocurrency blockchains, are inherently subject to a centralization risk that could lead to a 51% attack. Based on this, one could argue that 51% attacks are a known part of cryptocurrency investments and, therefore, investors should be considered to have consented to the risk of such an occurrence. But just because the occurrence of such an event is inherent and well known does not mean it is per se legal. For example, it is also well known and inherent in a cash-based system that someone can pickpocket one's wallet and gain access to all the cash inside. This is in no way an argument against the illegality of such behavior. One does not consent to losecash through pickpocketing simply because such an event is inherent to cash money and a well-known risk.

To support the assumption of risk defense to a 51% attack, one could attempt to analogize participating in a cryptocurrency market to that of participsting in games such as poker or Settlers of Catan. In these games, playersassume the risk that other players will attempt to use deception to deprive them of their in-game resources. And in Settlers of Catan, players enter the game assuming the risk that other players may collude in a common scheme to deprive them of their in-game resources. In both these examples, no crime has been committed because players willingly assume these risks when they agree to play the game. This analogy is further illustrative in that, if poker players and Settlers of Catan players used a threat of violence or hacked into a player's computer to gain an advantage, that would be illegal, just like with cryptocurrencies—if someone threatened violence or engaged in computer hacking to deprive someone of his or her cryptocurrencies, this would likewise be illegal. But, short of these intervening illegal actions, it could be argued under this theory that a 51% attack is not illegal.

There are other aspects of cryptocurrency that would strengthen the argument that people who choose to invest in it assume the risk of a 51% attack. Cryptocurrencies are well known for their association with illicit activities.[198] Governments have little control over cryptocurrency markets. Cryptocoins that are

---

[198] Michael Conklin & Ruben Ceballos, *The Ethics of Investing in Cryptocurrencies*, 21 FLA. ST. UNIV. BUS. REV. 69, 76 (2022).

stolen through explicitly illegal methods, such as threats of violence and hacking, are unlikely to be recovered.[199] And cryptocurrencies demonstrate very high market volatility. All of this common knowledge regarding cryptocurrencies could be interpreted to suggest that those who choose to ignore the warning signs and invest are assuming the risk that doing so in such a volatile, unregulated, unrecoverable, and illicit marketplace may result in a 51% attack.

A 51% attack was even warned about in Nakamoto's original paper introducing cryptocurrencies:

> The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.
>
> . . . If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.[200]

This acknowledgement of 51% attacks from the very inception of the first cryptocurrency could be used as evidence that anyone who buys into this marketplace assumes the risk. However, a counterargument could be made that Nakamoto's language used to describe such an attack implies a guilty mens rea and implies that such an occurrence is outside the boundary of what is acceptable for the marketplace. For example, he refers to the perpetrators as "attackers" that would need to overcome the "honest" miners. Other literature referring to a 51% attack describes the attackers as "bad actors."[201]

VIII. CONCLUSION

As demonstrated in this Article, the threat of cyberattacks and blockchain exploits is increasing at an alarming rate. Existing legislation—and related case law—was not written with such technologies, actions, or behavior in mind, leading to considerable uncertainty. Given the likelihood of a 51% attack, addressing the issue of potential legal recourse is as timely as it is consequential.[202] This Article provides a novel framework for analyzing criminal and civil causes of action for these attacks. By bringing these issues to light, cryptocurrency investors are better

---

[199] Gregory Bischoping, *Prosecuting Cryptocurrency Theft with the Defend Trade Secrets Act of 2016*, 167 UNIV. PA. L. REV. 239, 242 (2018).

[200] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* BITCOIN, 1, 3 https://bitcoin.org/bitcoin.pdf (last visited Dec. 24, 2022).

[201] *See, e.g.*, Randolph A. Robinson II, *The New Digital Wild West: Regulating the Explosion of Initial Coin Offerings*, 85 TENN. L. REV. 897, 913 (2018).

[202] *Cost of a 51% Attack*, *supra* note 169.

informed about the risks they are undertaking. Hopefully, this Article may also serve as a deterrent effect to those considering such an attack.[203]

The idea of a 51% attack is somewhat in its infancy, and analysis of the potential legal ramifications are even newer still. For example, a "Goldfinger attack" could be perpetrated by the government as a law enforcement tactic to reduce the illicit transactions that cryptocurrencies help facilitate. And given the rate at which the blockchain is evolving, new attacks not currently imagined are likely to emerge. This first-of-its-kind Article will hopefully serve as a valuable catalyst for future research in this evolving field. Recent dramatic price drops in cryptocurrency since 2021 function to make the likelihood of a 51% attack even more likely. This is because as mining becomes less profitable, the number of miners on a network falls. Fewer miners mean less hashing power, which makes it easier for an attacker to acquire the hashing power required to reach 51% of the entire network.

[203] Such a sophisticated attack would likely require significant collaboration and investment. This would likely increase the probability that legal experts would be consulted regarding the potential consequences of such an attack. This Article is a valuable resource for such legal experts.