FRAMING REGULATION AROUND THE POTENTIAL LIABILITIES OF PARTIES IN THE BLOCKCHAIN & SMART CONTRACT INDUSTRY

Jeceaca An[*]

ABSTRACT

Blockchains, which have been most significantly utilized by the technology, media, and telecommunication industry (TMT) and the financial sector, amassed global attention in the 2010s. This surging popularity may, however, cause the public to overlook the core characteristics of blockchain technology, and to consequently be unaware of the inherent risks at play when engaging with blockchains.

Simply put, blockchain technology is an information storing technology that can be utilized in various ways, such as services to facilitate cryptocurrency exchanges and smart contracts. The recent widespread use of blockchain technology by unique parties has raised questions of how to deal with the regulatory issues specific to the blockchain industry. This Note first identifies the significant parties in the blockchain and smart contract industry. This identification is crucial in determining the potential liabilities that could attach to each party.

Moreover, this Note recognizes that with greater use come greater issues. Recently, international and domestic jurisdictions have taken differing stances on regulatory frameworks to address the issues posed by blockchain technology. By virtue of the parties identified, this Note seeks to analyze the distinct approaches in determining the potential liabilities that should attach to blockchain administrators and its operatives to provide users and investors with better protections in light of recent events.

* J.D. Candidate, Fordham University School of Law, 2020; B.A. Chemistry, State University of New York at Geneseo, 2016. Thank you to everyone at the *Fordham Journal of Corporate & Financial Law* and Professor Mark Patterson for their valuable contributions in developing this Note. This Note is dedicated to my parents, James and Junghee An, and my sister, Jennifer An, for their special support throughout my life.

Blockchain users, its operatives, and participatory nodes are vulnerable to systemic failures, hacks, and errors that may have no available means for remedy. Despite the difficulties of advocating for regulation of the blockchain industry, this Note advocates for some degree of centralization, which should be an essential component of the regulation required to properly protect the involved parties and to allow growth in the industry.

TABLE OF CONTENTS

INTRODUCTION

Blockchains may completely change the way businesses operate; in fact, blockchains have begun to be implemented by more financial institutions and other commercial companies.[1] This widespread implementation may be due to the diverse applications available to business operations and the expected advantages resulting from such use in practice.[2] This emerging industry will heavily influence the global economy in the next few decades.[3] The blockchain industry is estimated to accumulate revenues of over $23.3 billion by the end of 2023.[4] However, the regulatory framework has yet to be formulated and "blockchain business development continues to outpace the regulatory process."[5]

Although blockchains have been in use for over a decade, the difficulty in unifying the regulatory framework remains due to the legal

1. *See generally* DEBEVOISE & PLIMPTON LLP, BLOCKCHAIN 2018 YEAR-IN-REVIEW (Feb. 14, 2019), https://www.debevoise.com/insights/publications/2019/02/blockchain-2018-year-in-review [https://perma.cc/56EK-JTSY] [hereinafter DEBEVOISE].

2. *Id.* Some applications include "physical asset traceability, clinical supply chain, global trade finance, cross-border payments and remittances, post-trade processing to voting and digital identity." DELOITTE, DELOITTE'S 2019 GLOBAL BLOCKCHAIN SURVEY: BLOCKCHAIN GETS DOWN TO BUSINESS (2019), https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf [https://perma.cc/A3A9-EEWW] [hereinafter DELOITTE'S BLOCKCHAIN SURVEY].

3. Shanhong Liu, *Blockchain Technology Market Size Worldwide*, STATISTICA (Aug. 9, 2019), https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/ [https://perma.cc/W87P-42SY]. *See also* DELOITTE'S BLOCKCHAIN SURVEY, *supra* note 2.

4. Liu, *supra* note 3, at 1.

5. Mary Thibodeau, *Self Regulation Goes Global for Blockchain Companies*, HEDGETRADE (Feb. 23, 2019), https://hedgetrade.com/blockchain-companies-try-self-regulation/ [https://perma.cc/T5PN-AXRN].

implications of its use.[6] Known legal processes may not fit the needs of the blockchain industry due to blockchain's decentralized nature and the broad scope of its new uses.[7] Thus, effective regulation would need to take the unpredictable nature of blockchain into account.[8] For example, self-regulatory bodies encourage decentralization and technological advancements,[9] whereas government agencies support stricter regulatory frameworks to reduce the risk of money laundering and fraud.[10] Since blockchains are used internationally, countries around the world are experiencing similar issues.[11]

An appropriate regulatory framework would give users and investors better protections by requiring parties to blockchain relationships and blockchain platforms to (1) establish control measures to authenticate the identity of financing users; (2) create a team of information technology (IT) specialists to oversee platform activity and provide users with complete and honest performance reports; (3) implement security systems that track abnormal activities (such as exchange hacking[12] or bugs in the system), comply with breach notification requirements, and permit write-in exceptions to reverse breach of theft in transactions, contracts, or information based on the magnitude of the breach; and (4) provide cyber insurance policies to all users and inform users of the risks associated with platform participation. Programmers should be subject to reporting requirements for identifying deceptive practices, training programs to

6. *See* DEBEVOISE, *supra* note 1, at 1.

7. GOV'T OFF. FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 6 (Jan. 19, 2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf [https://perma.cc/H3U2-JAER] [hereinafter DISTRIBUTED LEDGER TECHNOLOGY].

8. *See id.*

9. Andrej Zwitter & Jilles Hazenberg, *Decentralized Network Governance: Blockchain Technology and the Future of Regulation*, FRONTIERS IN BLOCKCHAIN (March 25, 2020), https://www.frontiersin.org/articles/10.3389/fbloc.2020.00012/full [https://perma.cc/T7Y4-CGP].

10. Matthew E. Kohen & Justin S. Wales, *State Regulations on Virtual Currency and Blockchain Technologies*, CARLTON FIELDS 2, 4, 10 (Aug. 29, 2019), https://www.carltonfields.com/insights/publications/2018/state-regulations-on-virtual-currency-and-blockchain-technologies [https://perma.cc/D478-CPHT].

11. *See* DEBEVOISE, *supra* note 1, at 1, 6, 20.

12. "An 'exchange hack' is theft of cryptocurrencies by malicious actors, otherwise known as hackers." *See* Jake Frankenfield, *Bitcoin Exchange*, INVESTOPEDIA (Dec. 2, 2019), https://www.investopedia.com/terms/b/bitcoin-exchange.asp [https://perma.cc/CB6L-M2RQ].

detect abnormal activity on blockchains, and coding practices that promote accuracy and coherence. Users must be informed of the risks involved in using blockchains—including the theft of information or cryptocurrency and the harm resulting thereof—and users should be insured to allow for recovery of harms.

This Note acknowledges the difficulties of regulating the blockchain industry. Nonetheless, blockchain users, its operatives, and participatory nodes are vulnerable to systemic failures, hacks, and errors that may have no available means for remedy. Some degree of centralization should be an essential component of blockchain regulation to properly protect the parties involved and to allow growth in the industry. Part I describes the nature of blockchain technology and identifies the parties involved in the industry. Part II discusses how current events illustrate the need for effective blockchain regulation and looks at the effect that regulations in other areas—including securities—have on blockchain. Part III first outlines the limitations in the current industry and advocates for some degree of centralization, and ultimately proposes a general regulatory framework. To provide users and investors with better protections, this framework suggests attaching liability to blockchain administrators and its operatives.

I. AN OVERVIEW OF THE BLOCKCHAIN AND SMART CONTRACT INDUSTRY

Part I of this Note is organized into three sections that illustrate the idiosyncrasies of the industry. The first section introduces blockchains and smart contracts and the novel functions of their technology. The second section attempts to identify the parties using blockchain. Due to the decentralized nature of blockchains, certain categories of parties may overlap, which may pose difficult regulatory issues. The third section focuses on domestic interests of the federal and state courts and identifies dominant regulatory actors that seek to acquire central control—or at least substantial influence—over the industry's regulatory developments in the United States. It then discusses the regulatory attempts made abroad by foreign actors and the practical and economic implications of such attempts.

A. INTRODUCTION TO BLOCKCHAIN AND SMART CONTRACTS

Blockchains are frequently outsourced and utilized by differing platforms.[13] Some platforms, such as Bitcoin, provide quick and easy transactions, while others, like Ethereum, enable the formation of contracts.[14] But as these platforms are gaining usership, many fail to understand the implications of the underlying technology.[15] While blockchain is commonly misconstrued to be exclusively financial, due in part to the prevalence of currencies like Bitcoin,[16] a blockchain is a de facto information storing device that operates at the hand of a hashing system.[17] An expansive range of information can be encrypted and recorded onto the blockchain, such as the details of financial transactions, terms of smart contracts, or raw data.[18] This capability is a foundational pillar of blockchain technology, which goes far beyond its mainstream recognition.[19]

The hashing system allows a block, illustratable as a "container data structure,"[20] to be attached to and recorded on a list of existing, verified blocks as soon as the block is verified by the first mining pool.[21] A mining

13. *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7, at 4–6, 8, 9, 34–35, 57. A blockchain is an information storing technology, comprised of unique blocks with recorded information about transactions. Companies use or administer blockchain technology for transactional services, such as cryptocurrency exchange platforms.

14. *See* Anthony Back, *What's the Difference Between Blockchain & Distributed Ledger Technology*, BLOCKCHAIN REV. 3–4 (Feb. 25, 2019), https://medium.com/blockchain-review/whats-the-difference-between-blockchain-distributed-ledger-technology-19407f2c2216 [https://perma.cc/U2DR-H52C].

15. Megan Ray Nichols, *10 Common Blockchain Misconceptions*, SCHOOLED BY SCIENCE 2, 4–5, 7 (Jun. 21, 2018), https://schooledbyscience.com/10-common-blockchain-misconceptions/ [https://perma.cc/L4PN-FU7Y].

16. *Id.* at 4.

17. Mark R. Patterson, *Blockchain Conceptual Primer*, LINKEDIN 1–2 (June 28, 2018), available at https://www.linkedin.com/pulse/blockchain-conceptual-primer-mark-r-patterson/.

18. *See* Back, *supra* note 14, at 2–3.

19. *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7, at 6, 9; *see also* Patterson, *supra* note 17.

20. Damien Cosset, *Blockchain: What is in a Block?*, DEV (Dec. 27, 2017), https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo [https://perma.cc/9Z9X-BEAN].

21. *See* Mehrdad Nojoumian, Arash Golchubian, Laurent Njilla, Kevin Kwiat, & Charles Kamhoua, *Incentivising Blockchain Miners to Avoid Dishonest Mining*

pool is a "joint group of cryptocurrency miners who combine their computational resources over a network."[22] Each block comprises a header, a list of transactional details, and a cryptographic hash—an inimitable identifier used to designate a particular block.[23] The transaction list identifies the miner who confirmed that particular block by its cryptographic address.[24] A miner is an individual user who actively participates on a blockchain by verifying and adding transactions to a public ledger.[25] The list also discloses that particular miner's transactional history, including the number of transactions the miner has participated in, the amount of blockchain sent and received from its address over time, and the current balance of its particular address.[26] Once a block is recorded onto the blockchain, the information incorporated therein is immutable and thus, cannot be erased or altered.[27]

A smart contract is a "self-enforcing" agreement that is managed by blockchain technology.[28] The smart contract consists of predetermined terms that are embedded in computer codes.[29] When two parties are in agreement on a smart contract, for example, the parties perform their contractual obligations, instantly triggering the execution of the contract, i.e., the transfer of money at a predetermined time or event.[30] By virtue of the underlying blockchain-management system, the stipulated terms cannot be altered and the contract cannot be expunged or modified.[31]

Strategies by a Reputation-Based Paradigm, ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING 1 (Sept. 8, 2017), http://faculty.eng.fau.edu/nojoumian/Files/Publication/MRepSR.pdf [https://perma.cc/26UA-MT9M].

22. Jake Frankenfield, *What is a Mining Pool?,* INVESTOPEDIA (Nov. 10, 2019), https://www.investopedia.com/terms/m/mining-pool.asp [https://perma.cc/W9PX-7QBL].

23. Cosset, *supra* note 20. *What are Cryptocurrency Miners? How does Cryptocurrency Mining Work?,* ETHOS (Mar. 2020), https://www.ethos.io/what-are-miners-cryptocurrency-mining [https://perma.cc/3UVY-HW5J].

24. *See* Cosset, *supra* note 20, at 5.

25. *See id.*

26. *See id.*; *see also* Patterson, *supra* note 17.

27. *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7, at 80, 83.

28. *See* Shermin Voshmgir, *Smart Contracts*, BLOCKCHAINHUB BERLIN 1 (July 2019), https://blockchainhub.net/smart-contracts/ [https://perma.cc/PGW9-XJWU].

29. *See id.*

30. Osman Gazi Güçütürk, *Smart Contracts and Legal Challenges*, MEDIUM (Aug. 2018), https://medium.com/@ogucluturk/smart-contracts-and-legal-challenges-1dcf306b98b8 [https://perma.cc/66D3-ZTD6].

31. *See id*.

B. PARTIES IN THE INDUSTRY

The decentralized nature of blockchain technology is largely responsible for its accumulating success. Blockchain-related interactions are generally between dispersed, remote, and, for the most part, anonymous parties—despite public disclosure of miner information in blocks. Some scholars consider decentralization to be the essence of blockchain use and contend that its protection is imperative to uphold the proper operation of blockchains.[32] Others disagree and contemplate the risks associated with this specific aspect of blockchains in light of new and unfamiliar circumstances.[33] This section identifies the different types of parties and categorizes them according to their respective goals. The parties of the blockchain industry fall into three broad categories: blockchain users, its operatives, and its participating nodes.

1. Blockchain Users

Blockchain users are predominantly companies. There are three types of companies that typically use blockchain; they are distinguished by the their (i) underlying purpose of implementing the blockchain, (ii) actual operational use of blockchain, and (iii) the service provided to end-users.

a. Blockchain Companies

A blockchain company refers to an entity that uses blockchain technology to encrypt its own sensitive and valuable information for storage, data analysis, or market strategy.[34] In place of the conventional record-keeping process—which requires paper, storage space, and

32. Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* (Dec. 1, 2015), https://ssrn.com/abstract=2709713 [https://perma.cc/KA5L-V2HN]; *see also* Hossein Nabilou, *How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency*, INT'L J. L & INFO. TECH. (Jan. 2019), available at https://www.researchgate.net/publication/332733039_How_to_Regulate_Bitcoin_Decentralized_Regulation_for_a_Decentralized_Cryptocurrency.

33. Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (Mar. 10, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [https://perma.cc/NBS7-R7VX].

34. *See generally* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.

periodic filing—companies may implement blockchain technology for overall efficiency in information storage and data analysis.[35] These companies incorporate the use of a permissioned ledger, which allows the blockchain administrator to select a handful of trusted actors to check the ledger's shared record.[36] This limited consensus process requires digital signatures to be viewable by all permitted parties for new records to be authenticated.[37]

b. Blockchain Platforms

A blockchain platform ("platform") employs blockchain technology to provide users with an interactive platform and a particular service.[38] These platforms employ an unpermissioned ledger, which invites anyone to access and contribute to the ledger.[39] Unlike permissioned ledgers, these ledgers do not have a single owner and "cannot be owned."[40] This system provides users with a public and verifiable way to maintain the ledger's record by majority consensus of the network.[41]

There are single-use public blockchains and multi-use public blockchains.[42] A single-use public blockchain is a public blockchain network.[43] For example, Bitcoin provides one specific function for payments and value storage: peer-to-peer (P2P) electronic payments.[44] A multi-use public blockchain can be both a public network and a developer network.[45] For example, Ethereum enables developers to build and deploy other decentralized applications ("dApps"), such as Bitcoin and EOS, to write and execute smart contracts.[46]

35. *See id.* at 5, 77, 80.
36. *Id.* at 7.
37. *Id.* at 5.
38. *See id.* at 17.
39. *Id.*
40. *Id.*
41. *See id.*
42. *Id.*
43. Back, *supra* note 14.
44. *Id.*
45. *Id.*
46. *Id.*

2. Blockchain Operatives

The blockchain industry requires a large base of experts who can adeptly operate the blockchain. These experts are distinguishable by the specific tasks they undertake.

a. Developers

A developer is a highly skilled programmer with an in-depth understanding of how blockchains work, who creates and updates blockchain software applications.[47] As developers continuously strive to develop more advanced software and technology to improve the security and efficiency of the blockchain system, groups of developers may create software applications to help with this task.[48] Software developments and updates require market research, data analysis, and coding experimentation.[49] Developers supervise the network and constantly experiment with existing data structures, such as merkle trees, to meet their personal network requirements.[50] These data structures are then applied with advanced cryptography to create blockchain systems with improved designs and greater security.[51]

b. Programmers

Programmers use blockchain technology to develop and create interactive interfaces for dApps.[52] In the context of smart contracts, programmers are increasingly relied on to provide dApps with legal templates and contractual terms that allow users to build and deploy their own smart contracts.[53] Programmers can also be miners, as discussed in

47. *See* Paul Aryya, *How to Become a Blockchain Developer? Types, Roles and Skills*, EDUREKA (May 22, 2019), https://www.edureka.co/blog/how-to-become-blockchain-developer/ [https://perma.cc/U9GT-8Z4P].

48. *See id.*; *see also Blockchain Technology Market Size, Share, & Trends Analysis Report,* GRAND VIEW RESEARCH (July 2019), https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market [https://perma.cc/L2RY-45Q7].

49. *Id.*; *see also Blockchain Developer: Salary & Job Description,* STUDY.COM (Apr. 25, 2018), https://study.com/articles/blockchain_developer_salary_job_description.html [https://perma.cc/9PDP-5JLH].

50. *Id.*

51. *Id.*

52. *Id.*

53. *See* Voshmgir, *supra* note 28.

Section B.3 below.[54] Notably, however, while miners verify and confirm blocks, they do not typically contribute to the actual codes.[55]

3. Participating Nodes

Platforms attract two types of "participating nodes," namely, computers run by miners and users.[56] Each node elects to participate on a platform due to the advantages provided by blockchains, such as reduced time and costs.[57]

a. Individual Users

Individual users ("users") are members of the public who participate on a platform.[58] A user can be a party holding digital wallets or a party to a smart contract.[59] These parties utilize the service of platforms to generate income or to access their information.[60] Users are attracted to platforms due to their quick financial returns, guaranteed security, and sheltered privacy.[61]

In addition, a user may have a financing purpose.[62] A financing user is an entity—such as an individual or corporation—that generates revenue by publicly seeking investments.[63] In cryptocurrency exchange platforms, a financing user can "advertise" a company on the platform and issue initial coin offerings (ICOs) or offer similar investment opportunities in order to acquire financing investments.[64]

---

54. *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.

55. *Id.*

56. *Id.*; *see also* Luke Fortney, *Bitcoin Mining, Explained*, INVESTOPEDIA (Nov. 6, 2019), https://www.investopedia.com/terms/b/bitcoin-mining.asp [https://perma.cc/4FP7-NPKX].

57. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.

58. *Id.*

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

63. *See Initial Coin Offerings (ICOs)*, SEC. EXCH. COMM'N (Apr. 11, 2019), https://www.sec.gov/ICO [https://perma.cc/8SJE-4NZN].

64. *See id.*; *see also* Jake Frankenfield, *Initial Coin Offering*, INVESTOPEDIA (Nov. 2019), https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp [https://perma.cc/K7R4-T6FC].

b. Miners

A miner is a user who is not employed by a particular entity but actively participates on platforms by coding its own transactions and encryptions onto blockchains. A miner presumably holds sufficient experience in coding, has a high degree of financial proficiency, and possesses a solid understanding of blockchains,[65] such that a miner could partake in more advanced modes of effecting financial transactions.[66] Miners also have the computational capabilities, including the power and software required to participate in transactions.[67]

Miners can be further distinguished as "honest miners" and "dishonest miners."[68] A dishonest miner hacks transactions, or even the blockchain itself, to steal money or information. Because blockchain activity is verified and established by the miners, the collective efforts of honest miners can impede the actions of dishonest miners before any harm is incurred.[69]

C. THE CURRENT REGULATORY STATE OF THE BLOCKCHAIN INDUSTRY

There are many moving parts in the blockchain and smart contract industry, creating issues that need to be addressed, such as the varying treatment of transactions by the legal and financial sector, the potential for business opportunities combined with market regulatory concerns, and the ability to manipulate blockchain technology to make illegal activities, such as money laundering, more difficult to detect.[70] Consequently, self-regulatory bodies, agencies, and federal and state

65. *See* Russell Brandom, *Why the Ethereum Classic Hack is a Bad Omen for the Blockchain*, THE VERGE (Jan. 9, 2019), https://www.theverge.com/2019/1/9/18174407/ethereum-classic-hack-51-percent-attack-double-spend-crypto [https://perma.cc/B227-M4BU]; *see also* ETHOS, *supra* note 23.

66. *See* Brandom, *supra* note 65; s*ee also* ETHOS, *supra* note 23.

67. Brandom, *supra* note 65.

68. Patterson, *supra* note 17.

69. *Id.*

70. Irena Asmundson & Ceyda Oner, *What Is Money?*, INT'L MONETARY FUND (Sept. 2012), https://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm [https://perma.cc/BX2H-CE9J]. *See generally* Matthew E. Kohen & Justin S. Wales, *State Regulations on Virtual Currency and Blockchain Technologies*, CARLTON FIELDS (Aug. 29, 2019), https://www.carltonfields.com/insights/publications/2018/state-regulations-on-virtual-currency-and-blockchain-technologies [https://perma.cc/6M37-XX3V].

courts currently approach the regulation of virtual currencies and blockchain technology with distinct perspectives.[71] The Virtual Commodities Association (VCA), a self-regulatory body comprising the industry's well-known organizations, believes blockchains should not be heavily regulated by governments and agencies and, instead, monitored for standard cryptocurrency trading patterns.[72] On the other hand, some states have attempted to treat all virtual currency operators as traditional money transmitters, which are covered by a restrictive regulatory framework under the Financial Crime Enforcement Network (FinCEN).[73] In addition, the New York State Department of Financial Services created "BitLicense," which requires all businesses related to transactions involving any form of virtual currency to obtain a license from the state in a stringent application process that includes "significant operational burdens."[74] In addition to reducing the risk of money laundering and fraud, regulators seek to safeguard the system against risks and market failure.[75]

Although not comprehensive, foreign countries may be ahead in framing the blockchain industry's regulation. The National Diet of Japan amended the Settlement Act and the Financial Instruments and Exchange Act ("FIEA") to require all Japanese cryptoexchanges and startups issuing a coin or token to comply with registration and disclosure requirements.[76] The new regulations aim to decrease fraud in the market by forcing providers to be accountable for exchange risks and ensuring reimbursement for certain user losses.[77] In Canada, new regulations target

71. *Id.*

72. Jordan French, *Can Self-Regulation Help Save the Cryptocurrency Market?*, THE STREET (Sept. 12, 2018), https://www.thestreet.com/investing/bitcoin/self-regulation-cryptocurrency-market-14696015 [https://perma.cc/SWV5-2WB7].

73. Kohen & Wales, *supra* note 10.

74. *Id.*; *see also* Sarah H. Brennan, *Contortions for Compliance: Life Under New York's BitLicense*, COINDESK (Jan. 22, 2018), https://www.coindesk.com/contortions-compliance-life-new-yorks-bitlicense [https://perma.cc/WZ79-AU2T?type=image].

75. *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.

76. *See* Makoto Koinuma, Koichiro Ohashi, & Yukari Sakamoto, *New Regulations in Japan on Security Token Offerings*, GREENBERG TRAURIG (July 24, 2019), https://www.gtlaw.com/en/insights/2019/7/new-regulations-in-japan-on-security-token-offerings [https://perma.cc/SN2B-M8XA]; *see also* Koichiro Ohashi, *New Regulations in Japan on Security Token Offerings*, NAT'L L. REV., July 24, 2019, at 2, https://www.natlawreview.com/article/new-regulations-japan-security-token-offerings [https://perma.cc/7K44-R53Y].

77. *See* Hisashi Oki, *Japan Hopes to Set Global Crypto Law Benchmark with Latest Regulatory Update*, COINTELEGRAPH (Jun. 5, 2019), https://cointelegraph.com/

those who are "engaged in the business of dealing in virtual currencies" by classifying domestic and foreign crypto platforms as money servicing business, which are required to implement compliance programs, register with the Financial Transactions and Reports Analysis Centre (FINTRAC), and to report any transaction valued over $10,000 in cryptocurrency with the transaction's details and the sender's identity.[78] Due to the infancy of these regulations, it is not yet certain how effective these regulatory attempts will be.[79]

II. THE POTENTIAL LIABILITIES OF PARTIES IN THE INDUSTRY

Blockchains allow platforms to provide users with opportunities to invest, contract, and store information.[80] In a perfect world, these opportunities are successful transactions.[81] However, in reality, a party may be harmed if the blockchain "fails." Blockchain "fails" may occur when "bugs" are embedded in the blockchain by manipulative users when they detect vulnerabilities in the system.[82] Dishonest miners can hack and manipulate the blockchain to steal information or money.

In the event of harm, a party may be uncertain of the available means to seek remedies under current regulations, as they do not outline the responsibilities of the parties. At first glance, it may seem obvious that users should be reimbursed for losses due to no fault of the user, such as thefts by dishonest miners. However, because of the decentralized nature of blockchain, the user may not be able to hold the miner responsible. The only remaining party is the platform through which the user's loss was incurred. Holding platforms responsible for all harms to users may be ethically unfair to platforms. Conversely, the absence of liability may have substantial effects on the formation and growth of the industry.[83]

---

news/japan-hopes-to-set-global-crypto-law-benchmark-with-latest-regulatory-update [https://perma.cc/6YJH-RKCT].

78. Daniel Palmer, *Canada's Crypto Exchanges Must Now Register as MSBs, Report Transactions Over $10K*, COINDESK (updated on July 11, 2019), https://www.coindesk.com/canadas-crypto-exchanges-must-now-register-as-msbs-report-transactions-over-10k [https://perma.cc/Q3BR-4J2J?type=image].

79. *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.

80. *See* Back, *supra* note 14.

81. *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7, at 8.

82. *See id.* at 78.

83. *See id.* at 74.

The following subsections divide and classify blockchain fails according to their nature by identifying the inflicting harms, the parties involved, and the underlying cause of the harm. Distributed ledgers and blockchains "share the same conceptual origin and purpose—a decentralized database or a log of records" and yet, they maintain "a distinct set of features."[84] Section II.A focuses on broader blockchain fails relating to the distributed ledger system, while Section II.B discusses the blockchain fails that may occur through user and content errors. Both parts seek to determine whether distinct regulatory frameworks shed light on formulating a framework for the industry at hand.

A. FAILS: DISTRIBUTED LEDGER TECHNOLOGY

A distributed ledger is "a database that is spread across multiple sites, countries or institutions."[85] Information is recorded and stored in a continuous ledger, one after another, "rather than sorted into blocks."[86] Moreover, a record can only be stored on the ledger when a quorum is reached by the parties, requiring a greater trust in the ledgers' operatives and users.[87]

Section A.1 first discusses errors made in virtue of distributed ledger technology and contemplates the comparison of the technology as a product and as the rules that regulate corporate operations. Section B.2 then discusses blockchain fails triggered by manipulation of the system—specifically, the 51 percent attack—which prompted further evaluation of the technology as a product, discussed in Section A.1, to address the results of a deceptive, external miner in the system and to determine the potential implications of product liability and breaching any fiduciary duties.

1. Software Errors

Suppose a company decides to implement a new software that will allow the platform to run double the amount of hashing that it currently does and accordingly, announces the new software update so that users can prepare for the system update. EOS, a blockchain-based, decentralized system that enables the development, hosting, and

84. Back, *supra* note 14.
85. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.
86. *Id*. at 17–18.
87. *See id.*

execution of commercial-scale dApps on its platform,[88] has a feature that requires all top twenty-one block producers to blacklist a certain account for the blacklist to function properly.[89] In February 2019, the EOS system update failed when one of the EOS block producers failed to synchronize the update with the other block producers.[90] As a result, an anonymous hacker was able to move 2.09 million EOS, the equivalent of $7.7 million, from a hacked account.[91] EOS responded with a proposal to nullify the keys of blacklisted accounts instead of providing a veto power to a single block producer on the main net, which fifteen out of twenty-one block producers approved.[92] There were three parties involved in this blockchain fail: the platform, the developers, and the users. The developers created a new software application and the platform attempted to implement the new software. The users presumably consented to the software update via a license during their time on the platform.[93] This creates a question as to whether the injured users have some type of remedy.

a. Distributed Ledger System as a Product

Distributed ledger technology and its updates are software applications comprised of a variety of codes.[94] Software applications are marketable products that can be created or purchased.[95] In a failed update, the hacked accounts are damaged and no longer viable.[96] There is also a loss of millions of dollars in cryptocurrencies, taken from hacked accounts.[97] Under product liability law, an injured party may seek

88. Shobhit Seth, *What is EOS?*, INVESTOPEDIA (Feb. 13, 2018), investopedia.com/tech/what-is-eos/ [https://perma.cc/2UQL-S7ZH].

89. Helen Partz, *Hacker Moves 2.09 MIn EOS following Blacklist Update Failure*, COINTELEGRAPH (Feb. 25, 2019). A block producer may blacklist a bad contract and every block producer has to fend off transactions that try to run that contract. This is the only way those transactions will not get into any blocks.

90. *See id.*

91. *Id.*

92. *Id.*

93. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.

94. Debevoise, *supra* note 1.

95. *See generally* Application Software 101, QUICK BASE (last visited March 31, 2020), https://www.quickbase.com/articles/application-software-basics#application-software [https://perma.cc/4C3Q-DTJK].

96. Partz, *supra* note 89.

97. *Id.*

damages under product liability when there is "an injury, harm, or damage due to a defective product."[98] The damages must result from "damage to or loss of the use of property, on account of any defect in any product which is manufactured, leased, or sold."[99] Additionally, damages caused by a defective product render any or all of the parties along the chain of manufacturing the product liable.[100] The imposition of product liability may be appropriate since it provides users with a concrete cause of action to seek remedies for damages incurred while using the platform.[101] In this instance, the developers are essentially manufacturers and the platform company is the distributor of the developed software. In the event of failure, platforms are likely to be liable since they provided the software application and the update. In addition, any legal cause of action that the platform company has against the developers could be made in a subsequent action, where the platform company may receive the proceeds directly from the developer.

Potential tort liability would require developers and platforms to use safer distributed ledger technology for platforms and their users.[102] However, product liability may not apply if the defect occurred during the installation of the product.[103] When a product and its related services are "integral parts of a transaction," the distributor or manufacturer must have actually relinquished control. In such cases, product liability applies to liabilities that arise "during the subsequent servicing of the product pursuant to a service agreement," where "initial delivery, installation, servicing, and testing" are completed.[104] Since the system update is user-effectuated, the damage may not be caused by a defect of the product, and is therefore not the fault of the platform or its developers.[105] Conversely, user installation is an obvious component of these products. Blockchain technology requires decentralized miners to work in the aggregate to verify and add any new blocks. For example, in a proof-of-work mining process, miners work in the aggregate to successfully process transactions

98. 26 C.F.R. § 1.172-13 (1986).
99. *See id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*
105. Partz, *supra* note 89; *see* Oscar Lage, Santiago de Diego, Borja Urkizu, Eneko Gómez & Iván Gutiérrez, *Blockchain Applications in Cybersecurity*, INTECHOPEN (Nov. 19, 2019), https://www.intechopen.com/online-first/blockchain-applications-in-cybersecurity [https://perma.cc/S3UP-WZTX].

or smart contracts.[106] Developers and platforms of such products would have to account for these defects in advance to ensure safe technology. To prevent software update defects, the platform can inform users of the requirements for a successful installation.[107] However, under the tort of product liability, platforms would only be liable for injuries resulting from reasonable, foreseeable risks—provided users are adequately warned.[108] In the blockchain context, though, adequate warnings may be difficult to provide, given its intangibility.

The tort of product liability may ensure that platforms employ blockchain technology that is capable of effectuating secure transactions. However, it is difficult to say whether permissioned or permissionless blockchain is the "best technology" from a security or privacy perspective.[109] Alternatively, developers may design around this defect to avoid liability altogether by creating software updates that do not require all miners to update software at the same time or design the system to prevent hacks in the event of an update failure.[110] This sort of technological sophistication would require developers and platforms to

106. Back, *supra* note 14.

107. *See* Partz, *supra* note 89; *see also* Lage, *supra* note 105 ("By providing information replicas and bringing closer the node that provides the service, the response time should be improved, and service outages avoided. But, how does that affect the information a customer can see? The Byzantine Generals Problem enunciated by establishes that the components of a distributed computing system may fail, reaching a condition of imperfect information. In this situation, an observer could have different information depending on unnoticed facts, like the server consulted or the client's location. A different observer could have different information for the same service consulted if an inconsistent CDN state is making the network to fail in its responses. A consensus regarding which component has failed in the first place and which information is trustworthy would make things easier.").

108. *See* Coulter Boeschen, *"Failure to Warn" in a Defective Product Case*, ALLLAW (last visited on Mar. 31, 2019), https://www.alllaw.com/articles/nolo/personal-injury/failure-to-warn-defective-product-case.html [https://perma.cc/72K6-YFEH] ("The warning . . . must be visible in a way that an expected user would see the warning. This means that some products are required to have a warning directly on the product itself, if the product is likely to be used by someone who will not see the packaging or have access to a manual."); s*ee also Legally Adequate Warning Labels: A Conundrum for Every Manufacturer*, FINDLAW (July 21, 2016), https://corporate.findlaw.com/litigation-disputes/legally-adequate-warning-labels-a-conundrum-for-every.html [https://perma.cc/63SU-L2YT].

109. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7, at 7.

110. *See generally id.*

create advanced technology in accordance to interoperability standards.[111] One way to achieve interoperable standards is for a private industry organization open to all companies to adopt a single standard.[112] Since the VCA aims to create industry standards, it may be willing to serve as the standard setting organization (SSO) to set standards for blockchain technology.[113] Moreover, in markets for complementary products, companies tailor their product to an industry standard.[114]

b. Distributed Ledger System as the Rules and Regulations

In another sense, software applications are not merely products. The applications' underlying codes dictate how the distributed ledger technology will run.[115] The codes control how the platforms operate and how the users operate. This process is analogous to the process by which corporations are regulated. A corporation's by-laws and articles of incorporation contain the rules and regulations that govern its operation.[116] The board of directors can amend the by-laws if the shareholders sign over their rights.[117] In the blockchain industry, the users essentially waive their rights to management on a decentralized platform. Similarly, the underlying software (regulations) does not change—rather, only additional codes (rules) are incorporated.

Ultimately, the board of directors creates and amends the by-laws for the benefit of the corporation and its shareholders.[118] The director's position is significant because directors must act in accordance with their fiduciary duties to exercise the duty of care in good faith when dealing with the management of corporate affairs.[119] At a minimum, the duty of care requires a general understanding of the corporation's affairs.[120] Similarly, the developers are tasked with creating and updating software

111. *See id.* at 14.
112. *Id.*
113. French, *supra* note 72.
114. Amrit Tiwana, *The Rise of Platform Ecosystems*, SCIENCE DIRECT (2014), https://www.sciencedirect.com/topics/computer-science/complementary-product [https://perma.cc/8XNM-PZNU].
115. *Id.*; *see* Andrew Meola, *Distributed Ledger Technology & the Blockchain Explained*, BUSINESS INSIDER (Jan. 16, 2020), https://www.businessinsider.com/distributed-ledger-technology-blockchain [https://perma.cc/8SF6-WU37].
116. 15 U.S.C. § 151.
117. 8 DCGL § 109(a).
118. Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. Supr. 1985).
119. *In re* Walt Disney, 906 A.2d 27, 30 (Del. 2006).
120. Francis v. United Jersey Bank, 87 N.J. 15, 31 (1981).

to fix systemic bugs and to provide greater efficiency, and the platform strives to provide those software applications to its users.[121] Treating the software application and its code as the rules and regulations of a corporation would put more responsibility on the platform and developers to provide users with more secure and safe transactions. As opposed to tortious liability, conveying the fiduciary duties owed by the board of directors of a corporation to the platform and developers of the blockchain industry may encourage parties to create secure technology that protects users' information. In the event that the board of directors breaches its fiduciary duties, the shareholders may pursue a derivative action, which cannot limit damages for acts carried out in bad faith.

2. System Manipulation

In a 51 percent attack, miners—which can be individuals or organizations—gain majority control of the network's mining power and prevent new transactions from gaining confirmations, which allows them to do the equivalent of writing a bad check.[122] On January 5, 2019, Ethereum Classic was hacked using the 51 percent attack.[123] A single entity gained control of approximately 60 percent mining power, giving them the ability to double spend by creating a longer blockchain.[124] The initial fraud reported was $460,000 and in the following days, the amount exceeded $1 million in fifteen different transactions.[125] It took twenty-four hours for Coinbase, a prominent cryptocurrency platform, to take notice.[126]

Traditional payment systems are administered by financial institutions. These institutions serve as gatekeepers at each end of the transaction, verifying the availability of funds before disbursing, and vice versa, to prohibit double spending.[127] Although blockchains are programmed to impede double-spending, there is no central authority in unpermissioned distributed ledger systems held responsible if double-

121. Aryya, *supra* note 47.
122. Brandom, *supra* note 65.
123. *Id.*
124. Gina Clarke, *After Ethereum Classic Suffers 51% Attack, Experts Consider–Will Bitcoin be Next?*, FORBES (Jan. 9, 2019).
125. Brandom, *supra* note 65.
126. Clarke, *supra* note 124.
127. Brandom, *supra* note 65.

spending does occur.[128] Requiring the platform to act like a financial intermediary would not resolve the double-spending issue because cryptocurrency transactions are enforced through a distributed ledger that is collectively produced by currency miners.[129]

a. Product Liability

The 51 percent attack was unique because the attack was on the blockchain itself and the blockchain was, in fact, rewritten.[130] Because blockchains guarantee immutability, the blockchain itself fails in these instances.[131] In other words, the blockchain may have been defective. The defect would have also certainly caused damage to or loss of the use of property to its users.[132] In contrast to the implementation of a software application or an update, users are significantly harmed without having made any errors.[133] The potential liability of platform companies and developers may be appropriate given that these parties are required to ensure safe distributed ledger systems for consumers.

On the other hand, product liability for defects caused by attacks on the blockchain may be unfair to developers and may unduly burden development.[134] The manufacturers and distributors are only liable for offering a defective product to the general public—i.e., consumers.[135] Liability may not be appropriate in cases of hacks given that the liability arises during the service of the products.[136]

b. Breach of Fiduciary Duties

The platform may be viewed as a typical corporation from the perspective of shareholders. In a corporation, the board must perform duties of good faith with the degree of care that an ordinarily prudent person in a like position would use under similar circumstances.[137] In the blockchain and smart contract industry, the platform is essentially the

128. *Id.*
129. *Id.*
130. Clarke, *supra* note 124.
131. *Id.*
132. *Id.*
133. *Id.*
134. Kohen, et al., *supra* note 10.
135. *See* 26 C.F.R. § 1.172-13 (1986).
136. *Id*.
137. Francis v. United Jersey Bank, 87 N.J. 15, 28 (1981).

corporation.[138] Although there are no directors or shareholders, the platform has the developers and programmers.[139] The corporation has a duty to supervise corporate performance and to establish monitoring systems and must, in good faith, believe that the systems are sound in design and operation.[140] Fiduciary duties relevant to our analysis include the duty to inform shareholders of material changes to the corporation on a perpetual basis and to act in the interests of the shareholders.[141]

In the 51 percent attack, the duty to provide safe technology was breached because the technology had already failed. Moreover, the attack was not completely unanticipated.[142] Cryptocurrency developers had known similar attacks were possible for a long time due to the increase of available, cost-efficient mining equipment.[143] Moreover, these attacks are predicted to become more common, as equipment is expected to become cheaper and therefore, more easily accessible to miners.[144] It is also known that smaller coins like Ethereum Classic, as opposed to major coins such as "mainline Ethereum," are inherently vulnerable with an increasing risk.[145] Because hackers can reap high rewards by attacking even small cryptocurrencies, smaller cryptocurrencies may need different encryption algorithms than those employed by bigger ones.[146] Bitcoin is unlikely to be vulnerable to an attack because it has a large enough mining power to resist 51 percent attacks and uses a chip-specific protocol, making it less responsive to repurposed equipment.[147] However, current cost estimations predict that it would take "just over $520,000 to take control of the Bitcoin network for a solid hour."[148]

The fiduciary duty to employ technology in the shareholders' best interests may be burdensome on directors since they have to predict

138. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.
139. Aryya, *supra* note 47.
140. *Id.*
141. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 409, 116 Stat. 745 (2002) (prior to 2010 amendment).
142. Brandom, *supra* note 65.
143. *Id.*
144. *Id.*
145. *Id.*
146. David Canellis, *Cryptocurrency Hackers Earned $20M With 51-Percent Attacks In 2018*, THE NEXT WEB (last visited Feb. 11, 2020), https://thenextweb.com/hardfork/2018/10/23/cryptocurrency-51-percent-attacks/ [https://perma.cc/57MN-ZA8E].
147. Brandom, *supra* note 65.
148. Canellis, *supra* note 146.

unknown risks,[149] which requires expertise in blockchain technology and how they operate. A director's fiduciary duties require her to make informed decisions.[150] In this determination, directors are able to defer and rely on statements of experts.[151] Platforms may be informed of the risks associated with the technology by developers—the "informed players."[152] The platforms likely require multiple sources of advice.

To address systemic failures of corporations, Congress set forth the minimum standards for professional conduct for lawyers to prevent fraud and conspiracy.[153] SEC Rule 205 treats attorneys as "gate keepers" and requires issuers' attorneys to internally report "evidence of material violation" of security laws, a material breach of fiduciary duty, or a similar material violation by the company "that has occurred, is occurring or is about to occur."[154] The rule's objective of deterring fraud, protecting investors, and increasing investors' confidence in public companies is in line with the SEC's objective.[155] A reporting requirement may be appropriate because it would require the platform to monitor its blockchain and address any material breaches or violations. Moreover, it took twenty-four hours to notice over $1 million lost in fifteen different transactions from the 51 percent attack on Ethereum.[156] Under SEC Rule 205, an attorney must first report her findings to the audit committee. If she believes that an appropriate response was not provided within reasonable time, the attorney must then report her findings to the board of directors.[157] Subsequently, the attorney has the discretion to "report out" to the SEC if the highest authority fails to address a clear violation of the law and the attorney reasonably believes that the violation is reasonably certain to result in substantial injury to the issuer.[158]

149. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.

150. Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. Supr. 1985).

151. *Id.* at 33.

152. Aryya, *supra* note 47. See TONY UCEDAVELEZ & MARCO M. MORANA, RISK CENTRIC THREAT MODELING: PROCESS FOR ATTACK SIMULATION AND THREAT ANALYSIS 331 (2015).

153. *SEC Standards*, DAVIS POLK & WARDWELL LLP (July 3, 2003), https://www.davispolk.com/files/07.03.sec.standards.prof.conduct.pdf [https://perma.cc/Z374-VUYR].

154. *Id.*

155. SEC Rule, 17 C.F.R. § 205 (2003).

156. Clarke, *supra* note 124.

157. SEC Rule, 17 C.F.R. § 205 (2003).

158. *Id.*

A developer would not have received feedback from any higher-ranked groups, specific to the blockchain industry, while an attorney would be obligated to report the material violation to the company's chief legal officer, the audit committee, and the board of directors.[159] At this point, the attorney has advised the board of directors of the substantial injury that is reasonably certain to occur to the issuer.[160] If the board of directors chooses to disregard a clear violation of the law, the issuer and the board will assume the resulting liability or criminal sanctions.[161] The legal officer and the directors are professionals who are trained to assess the issue from an objective point of view.[162] These parties are able to investigate the potential violation, determine the likelihood of substantial injury, and retroactively correct any violations that may have occurred.[163] Conversely, users do not have comparable expertise or resources available to them. The requirement to "report out" may not be effective since most programmers are miners. It would be ineffective to mandate miners to report such activity to a higher authority because there is no way to verify whether miners are actually monitoring all activity on the blockchain.

A platform's treatment as a corporation may not adequately encompass the decentralized nature of the parties in the industry.[164] If the platform's monitoring system, implemented to ensure a system's security measures meet a "good faith standard" monitored performance accordingly, the users may not be able to recover the losses incurred from an attack.[165] However, the losses will already have been incurred and the user will already have been harmed. Because miners are hacking a distributed ledger system, their identities may not be traceable and there may not be an appropriate party to attach liability.[166] Even if the platform comprehensively monitors the blockchain, there may be abnormal activities that are unrecognizable at first sight.[167] While the nature of

159. *Id.*
160. *Id.*
161. *Id.*
162. *Id.*
163. *Id.*
164. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.
165. Smith v. Van Gorkom, 488 A.2d 858, 872–73 (Del. Sup. Ct. 1985).
166. Brandom, *supra* note 65.
167. Shannon Wu, *The Most Lucrative ETH Scams, Top-to-Bottom*, BLOOM (June 24, 2018), https://bloom.co/blog/the-most-lucrative-eth-scams--top-to-bottom-/ [https://perma.cc/SES2-3SF2].

blockchains makes new attacks and the resulting losses inevitable, losses may be manageable.[168] Although it took twenty-four hours to notice the 51 percent attack, discussed in Section A.2, the majority of the losses were stolen over a number of days and traced back to fifteen different transactions. Identifying and reversing just a few of those transactions could have saved half a million dollars. To reduce the losses incurred from an attack, the platform would have to institute an exception to the immutability of blockchains and "write-in" lines of codes to reverse transactions. Given the control settings of the blockchain, however, the system would first need to be modified to grant access permission to certain administrators.

B. FAILS: THE BLOCKCHAIN

A blockchain is "a specific type of distributed ledger."[169] The blockchain employs a system that hash-links blocks in a sequential chain, requiring user consensus, and "organizes data in blocks, and updates the entries using an append-only structure."[170] As discussed in Part I.B.1, blockchains can be distinguished by their actual use. Part II.B identifies the harms that may occur in single and multiple use blockchains and determines the potential implications in light of rules and regulations, including Generally Accepted Accounting Principles (GAAP), the Communications Decency Act of 1996 (CDA), and the Securities Exchange Act of 1934.

Section B.1 first introduces the effect of errors made in content and contemplates the comparison of a platform's content and its blockchain to a financial statement. It further considers the source of the content, the platform, its operatives, or the users—that is, who creates the content and uses the available tools. Section B.2 then discusses fraud perpetrated through content errors, specifically in initial coin offerings, causing stricter review of content as a service or a tool, under section 230 of the CDA, and additional considerations on the potential implications of securities regulation in the blockchain industry.

168. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7; *see also* Julia Magas, *Crypto Exchange Hacks in Review: Proactive Steps and Expert Advice*, COINTELEGRAPH (Aug. 31, 2018), https://cointelegraph.com/news/crypto-exchange-hacks-in-review-proactive-steps-and-expert-advice [https://perma.cc/NP54-LDUB].

169. Back, *supra* note 14.

170. *Id.*

1. Content Errors

Suppose two users, X and Y, enter into a smart contract. X performs but does not receive money from Y, which may be due to a coding error.[171] In fact, the most common "bug" found in contracts is wrongly-named constructors.[172] A constructor is a special function, which runs when the program starts,[173] and must have the same name as the contract.[174] Otherwise, "the contract can be called by anybody" and any user can become the new owner of the contract and withdraw the money.[175] Here, the users are harmed with the loss of money or information.

As blockchain technology expands, its advocates suggest efficiency as one of its key advantages.[176] There is no longer a need to receive bank approval for a financial transaction or to retain an attorney to draft a contract.[177] By cutting out the middle-man in these transactions, platforms provide faster transactions and reduced costs. However, there is one middleman: the programmer.[178] Suppose now that two users agree on a smart contract agreement. The smart contract comprises contractual terms found on the platform. However, the contract contains erroneous content. There are two potential sources of error: (1) the programmer who provided the dApp for users to build and deploy their own contracts; and (2) the miners who created and uploaded the content on the network.

a. Blockchains as Financial Statements

The transactions recorded on the blockchain reflect the platform's history. The blockchain records transactions, like a receipt. Essentially, each block is a journal entry[179] that provides complete information with respect to a transaction.[180] Similarly, each block recorded on the

171. *How to Steal Ethers: Scanning for Vulnerable Contracts,* PALKEO (Dec. 5, 2018), https://www.palkeo.com/en/projets/ethereum/stealing_ether.html [https://perma.cc/S8RT-VSDU] [hereinafter *How to Steal Ethers*].

172. *See id.*

173. *Id.*

174. *Id.*

175. *Id.*

176. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7, at 58–59, 80.

177. *Id.* at 83.

178. Aryya, *supra* note 47.

179. STEPHEN H. BRYAN, FUNDAMENTALS OF FIN. ACCT. AND ANALYSIS 6 (6th ed. 2018).

180. Cosset, *supra* note 20.

blockchain provides the details of the transaction. Journal entries are recorded in a journal, containing "the data about the transactions that eventually are incorporated into financial statements."[181] In the blockchain industry, no party is liable for the proper identification, valuation, recording, and disclosure of the events.[182]

In a traditional setting, accountants prepare financial statements to inform the public of a company's financial position in accordance with GAAP.[183] Since investors rely on these statements to make informed investment decisions, accountants must carefully prepare a company's financial statements to provide an honest and complete disclosure of the company's operations.[184] Additionally, financial statements must be audited by an independent auditor and subsequently affirmed by the company.[185] An accountant's error in a financial statement may call for liability, depending on the scope of the error.[186] Accountants may raise an affirmative due diligence defense to avoid liability and as an expert, the accountant would be held to GAAP standards.[187] Accordingly, programming and accounting may not be identical because accountants may not be liable for errors in the financial statement, so long as GAAP was followed.[188] In the event that the accountant is not liable for misstatements made in the financial statement, the injured investors may seek damages against the issuer and any other party who signed the registration statement but failed the due diligence test.[189]

In contrast, in the blockchain and smart contract industry, injured users do not have such remedies available to them. The lost accounts, money, and/or information inflict direct harm that may not be accounted for due to the decentralization of users.

---

181. *See* BRYAN, *supra* note 179, at 6.

182. AICPA, BLOCKCHAIN TECHNOLOGY AND ITS POTENTIAL IMPACT ON THE AUDIT AND ASSURANCE PROFESSION (2017), https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf [https://perma.cc/Z2BU-578A].

183. *See* BRYAN, *supra* note 179, at 3.

184. 15 U.S.C § 7201 (2002).

185. Bryan, *supra* note 179.

186. 15 U.S.C. § 77k (amended 1995).

187. Bryan, *supra* note 179; *see also* William K. Sjostrom, Jr., *The Due Diligence Defense Under Section 11 of the Securities Act of 1933*, 44 BRANDEIS L. J. 549, 598–99 (2006).

188. *See id.*; *see also* AICPA, *supra* note 182.

189. 15 U.S.C. § 77k (amended 1995).

b. Blockchains as Legal Agreements

Certain programmers may be tasked with creating contractual terms that are provided to smart contract users.[190] These programmers, like accountants, carefully prepare the code to be used in smart contracts.[191] However, unlike accountants, programmers deal with legal concepts,[192] as they are required to translate known legal concepts into encrypted terms that are readily usable in smart contracts—an undertaking conventionally assumed by a lawyer.[193] Because parties are legally bound by contracts, lawyers are expected to draft contracts with great care and to inform clients of the rights and obligations entitled to each party.[194] In the event that a lawyer includes a faulty work or fails to accurately convey the implications of the terms, the client has the right to bring an action for malpractice.[195] In this regard, a programmer's role is increasingly relied upon to provide users with readily usable dApps with accurate translations of law into code.[196] Even if programmers improved the accuracy of materials, there are still injuries resulting from users' failures to fully understand the legal implications of the contractual terms.[197] Although current smart contracts are generally straightforward and unadorned of complex legal terms, platforms may eventually provide complicated legal materials that may be unintelligible to users.[198]

190. Aryya, *supra* note 47.

191. *Id.* 47 U.S.C. § 230 (2018) (An access software provider is a "provider of software (including client or server software), or enabling tools . . . .").

192. Voshmgir, *supra* note 28.

193. Jeffrey D. Neuburger, Wai L. Choy & Kevin P. Mileswski, *Smart Contracts: Best Practices*, PROSKAUER ROSE (2019), https://s3.amazonaws.com/assets.production.proskauer/uploads/dc2c188a1be58c8c9bb8c8babc91bbac.pdf [https://perma.cc/ZHE9-UT3S].

194. Gregory M. Duhl, *The Ethics of Contract Drafting*, 14 LEWIS & CLARK L. REV. 989 (2010); MODEL RULES OF PROF'L RESPONSIBILITY, Preamble, r. 2.1 (AM. BAR ASS'N 1983).

195. Charles F. Krause & Alfred W. Gans, *Generally; negligence; professional skill, prudence, and diligence*, 4A AM. L. TORTS § 15:82 (last updated March 2020).

196. *See generally* Neuburger, *supra* note 193. *See also* Richard Chen, *A Brief Overview of dApp Development*, MEDIUM (March 5, 2018), https://thecontrol.co/a-brief-overview-of-dapp-development-b8ac1648322c [https://perma.cc/U9UG-SAJ7].

197. *See* Neuburger, *supra* note 193.

198. Craig Sproule, *As Smart Contracts Get Smarter, the Rules of Development will Change*, VENTURE BEAT (Feb. 18, 2018), https://venturebeat.com/2018/02/18/as-smart-contracts-get-smarter-the-rules-of-development-will-change/ [https://perma.cc/GG67-MPSN].

Currently, requiring programmers to act like accountants and lawyers may not be advisable because programmers are not regulated, licensed specialists.[199]

c. Blockchains as Services or Content

On some platforms, content is created solely by users. The public network merely provides users with the tools to carry out their individual endeavors, such as writing and executing a smart contract. However, in many cases, platforms facilitate programmer or user-generated content. A closer look reveals that single-use public blockchains essentially resemble interactive computer services, which are "information service[s], system[s], or access software provider[s] that provide[] or enable[] computer access by multiple users to a computer server."[200] For example, Bitcoin provides one specific function—P2P electronic payments—for payments and value storage.[201] Under the CDA, providers are given a broad immunity, limiting third-party content moderation. A multi-use public blockchain, such as Ethereum, would be considered an information content provider if it was responsible for the creation or development of the information provided on the internet.[202] However, Ethereum is an open-source platform for decentralized applications.[203] The creators of the software make the source code available for anyone to copy or alter.[204]

Generally, service providers are immune from liability under Section 230 of the CDA as long as they do not contribute to any alleged illegality and do not develop or create information.[205] Alternatively, service providers may be liable if they compile false or misleading content.[206] Operators who edit user-created content are directly involved in the alleged illegality; for example, by "transform[ing] an innocent message into a libelous one."[207] In the context of smart contracts, programmers who make errors in user transactions transform correct messages into

199. Aryya, *supra* note 47. *See generally* AICPA, *supra* note 182.
200. 47 U.S.C. § 230 (2018).
201. *Id.*
202. Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 717 (Cal. 2002).
203. ETHEREUM, http://ethereum.org (last visited Feb. 11, 2020).
204. *What is Open Source Software?*, OPEN SOURCE, https://opensource.com/resources/what-open-source (last visited Dec. 28, 2019).
205. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1168 (9th Cir. 2008).
206. *Gentry*, 121 Cal. Rptr. 2d at 718.
207. *Roommates.com*, 521 F.3d at 1169.

wrong or inaccurate records.[208] These edits result in the execution of an "erroneuous smart contract," causing the loss of information or money.[209] The characterization of a coding error is unlikely to constitute an illegality.

2. Fraudulent Content

Suppose a user finds an appealing investment opportunity on a platform that requests the user to invest a small amount of money for future profit. In this type of situation, users should be wary of "honeypots," which are bugs found in vulnerable contracts, where the user sends the money but never receives a return.[210] Here, malicious actors take advantage of users by appealing to them with the keyword "give."[211] Instead of returning the promised profit, the contract keeps the money sent. Suppose, in another instance, a user decides to invest in an ICO and deploys a token contract with the associated token sale. The ICO turns out to be fake and the user ends up losing all associated coins.[212] In fake ICOs, miners go as far as creating fake profiles and websites to attract and scam investors.[213]

In a traditional system, parties are better protected against fraud because financial intermediaries verify the availability of funds before disbursement. Individuals are generally responsible for their business decisions. In honeypots and fake ICOs, users' affirmative decisions cannot be informed.[214] Users are investing in something that does not exist.[215] With that said, bugs found in vulnerable contracts are identifiable.[216] However, many users may not be educated in distinguishing between legitimate and fraudulent investment opportunities.[217] In addition, the scams reported on EtherscamDB—an open-source dataset that tracks malicious URLs and their addresses—amounted to estimated losses of $23 million to scams with confirmed

208. *See* Neuburger, *supra* note 193.
209. *Id.*
210. *How to Steal Ethers*, *supra* note 171.
211. *Id*.
212. *Id.*
213. *Id.*
214. *Id.*
215. Wu, *supra* note 168.
216. *How to Steal Ethers*, *supra* note 171.
217. DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 7.

addresses, which are addresses associated with scams, traced by a scam scanner.[218] There are thousands of other scams on EtherscamDB that do not have confirmed addresses associated with them. Reliable and comprehensive information on the magnitude of fraudulent activity is lacking.

a. Communications Decency Act § 230

Under Section 230 of the CDA, providers are given a broad immunity, limiting third party content moderation, to promote the constitutional right of free speech to express political opinions and personal views.[219] Due to the immense volume of activity on websites, operators are not required to actively investigate all activity.[220] Requiring platforms to actively investigate all activity may be similarly futile. Blockchains have an immense volume of activity, particularly single-use public networks. In Bitcoin, for example, a block contains more than 500 transactions.[221]

The imposition of content monitoring may be difficult to enforce due to the many limitations inherent in blockchains, such as the decentralized nature of blockchains and its users. Additionally, self-regulated bodies seek to keep regulations away from the blockchain industry to uphold decentralization. Likewise, in the internet industry, broad immunity limits third party content moderation.[222] However, even with these persuasive rationales, internet companies must be able to provide legitimate content.

In *HomeAway.com, Inc. v. City of Santa Monica*, an ordinance required platforms to authorize transactions for only those involving licensed properties.[223] The platform argued that the ordinance forced them to monitor and remove third party content. However, the ordinance did not "discuss the content of listings that the platforms display" and only prohibited the processing of transactions for unregistered properties.[224] The "monitoring" of the property registry could not constitute "publication of third party content" when platforms have no editorial

218. Wu, *supra* note 169.
219. 47 U.S.C. § 230 (2018).
220. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008).
221. Cosset, *supra* note 20.
222. HomeAway.com, Inc. v. City of Santa Monica, 918 F.3d 676 (9th Cir. 2019).
223. *Id.* at 687.
224. *Id.* at 682.

control over the registry.[225] The platform also argued that the ordinance contradicted the CDA's policy to allow internet technology and the market to expand with minimum interference of federal and state regulations.[226]

The VCA would likely agree with the platform's argument to leave the industry "unfettered by Federal or State regulation."[227] Notably, courts dismissed arguments that render unlawful conduct to be "magically . . . lawful when [conducted] online," to give "online businesses an unfair advantage over their real-world counterparts."[228] Subjecting IPO issuers to substantial disclosure requirements while imposing few, if any, on ICO issuers may give illegitimate ICO issuers an unfair advantage over traditional issuers.[229] Any attempts to regulate the blockchain industry by requiring users of ICOs to disclose information to governments and agencies will be likely viewed as a step away from decentralization.[230]

b. Securities Regulation

Initial offerings are significant in that the public may purchase shares in a particular company for the first time.[231] Issuers—which are legal entities that develop, register, and sell securities to finance their operations—are required to register offerings, disclose significant financial information, and follow stringent disclosure timelines.[232] These entities are legally responsible for the disclosure of the issue and must comply with the reporting obligations relating to financial conditions,

225. *Id.* at 682–83.

226. *Id.* at 681.

227. French, *supra* note 72.

228. *HomeAway.com*, 918 F.3d at 683.

229. Note that ICO issuers have been subjected to enforcement actions by the SEC and have, in some circumstances, been placed on a level playing field with traditional issuers. See *Cyber Enforcement Actions*, SEC, (last updated Mar. 23, 2020), https://www.sec.gov/spotlight/cybersecurity-enforcement-actions [https://perma.cc/Y6C5-QN4H].

230. Tyler Whirty, *Protecting Innovation: The Kin Case, Litigating Decentralization, and Crypto Disclosures*, ALT+M (Feb. 1, 2019), https://www.alt-m.org/2019/02/01/protecting-innovation-the-kin-case-litigating-decentralization-and-crypto-disclosures/ [https://perma.cc/Q43D-M2L9].

231. Adam Hayes, *Initial Public Offering (IPO)*, INVESTOPEDIA (Apr. 28, 2020), https://www.investopedia.com/terms/i/ipo.asp [https://perma.cc/M2UX-5E47].

232. 15 U.S.C. § 77k (2012).

material developments, and other operational activities.[233] Disclosures must include audit reports of financial statements by an independent auditor.[234] Auditors must comply with general auditing standards and procedures under the purview of the Public Company Accounting Oversight Board (PCAOB).[235] Issuers are trusted to properly inform prospective investors given that untrue or misleading disclosures can result in civil and criminal sanctions.[236]

In the blockchain industry, financing users of ICOs act like issuers. Financing users seek investments in initial offerings. Although initially unclear, most coins generally fall within the scope of securities,[237] and coin offerings are made to the public in the same manner as securities offerings. The financing user (an issuer) presents platform users (the public) with the opportunity to purchase (or invest in) coins (securities) for the first time in an ICO. Unlike issuers, however, financing users are not faced with stringent disclosure requirements and potential criminal sanctions.

The absence of disclosure requirements and liabilities may provide financing users with an unfair advantage over their "real-world counterparts," the issuers, due to financing users' ability to disclose false information—such as a nonexistent contact—and circumvent the costs associated with registration and reporting requirements. Because users are decentralized and unmonitored, it is nearly impossible to distinguish legitimate financing users from manipulative users who create fake company profiles to scam users in ICOs. Disclosure requirements may decrease the number of fake ICOs since fraudulent coin offerings can be tied to the financing user and allow users to make informed decisions. Any offering of securities, not including derivatives and futures contracts, is under the SEC's jurisdiction. Putting aside disclosure requirements mandated by SEC regulations, the blockchain industry does not have a

233. PRINCIPLES FOR ONGOING DISCLOSURE AND MATERIAL DEVELOPMENT REPORTING BY LISTED ENTITIES, SEC (Oct. 2002), https://www.sec.gov/about/offices/oia/oia_corpfin/princdisclos.pdf [https://perma.cc/CL5B-59VR] [hereinafter PRINCIPLES FOR ONGOING DISCLOSURE].

234. AUDITING STANDARDS, PCAOB (2017), https://pcaobus.org/Standards/Auditing/Pages/AS3101.aspx [https://perma.cc/4FQC-TLEH].

235. *Id*.

236. *See* PRINCIPLES FOR ONGOING DISCLOSURE, *supra* note 233.

237. *See* SEC RELEASE NO. 81207, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf [https://perma.cc/9Y45-XUJY].

central authority requiring financing users to disclose information.[238] Disclosure requirements may be difficult to enforce in the blockchain industry due to the influence of self-regulating bodies to keep platforms decentralized. With that said, disclosure requirements have the power to decrease fraud and promote transparency.

III. PROPOSITIONS FOR REGULATORY FRAMEWORK

Current regulatory approaches do not focus on the combination of the nature of blockchains, the parties of the industry, and the potential liabilities of such parties. The blockchain and smart contract industry requires some degree of centralization to provide parties with protection and realistic means to seek remedies. This would require a regulatory framework to impose responsibilities on the parties and to hold such parties liable in the event of failure. Three focuses were discussed in Part II of this Note: the security of utilized technology and an established system, the accuracy of provided content, and the protection of users.

Secure Technology and Sound Systems. A duty to disclose should be implemented in order to incentivize platforms and developers to provide users with safer platforms to engage in activity. The software applications that developers create and platforms employ is the technology on which users rely. In sum, blockchains need to provide a safe environment for users to interact.

Accurate and Honest Content. The programmers' role in the blockchain industry is growing, and an ideal regulatory framework would hold programmers accountable. Programmers should be required to act in accordance with some sort of heightened duty to provide users with accurate legal materials and protect any sensitive and valuable information. Additionally, since smart contracts require the use of legal knowledge and interpretation, blockchain and smart contract programmers should be held to a higher standard than ordinary programmers. Requiring programmers to act in accordance with

238. While there is no central authority, the blockchain industry must at least follow SEC disclosure requirements, and blockchain companies may face liability even if they use an exemption to offer securities (should they fail to adhere to each exemption requirement). For example, Telegram Group used a private placement exemption, but still encountered a TRO. Telegram Group is currently fighting in court with the SEC. Complaint, SEC v. Telegram Group, 19 Civ. 9439 (PKC) (S.D.N.Y. Oct. 11, 2019), https://www.sec.gov/litigation/complaints/2019/comp-pr2019-212.pdf [https://perma.cc/F34S-4WVK].

heightened duties would undoubtedly increase the accuracy of content created on platforms. Although errors cannot be completely eliminated, users should be aware of platform performance in this regard. Users may elect to use one platform over another if they are aware of better performance and minimal errors or fails.

The blockchain industry processes immense volumes of information that is accessible to millions of users.[239] These users, in turn, either use such content or rely on such information in making transactional decisions. Platforms should not be restricted in order to allow some degree of decentralization to be upheld in the blockchain and smart contract industry. However, potential liability for platforms should not be hastily abandoned. Users should be able to seek redress in circumstances of fraud. Disclosure requirements may be difficult to enforce due to the interests of self-regulating bodies to keep platforms decentralized. However, it may be necessary to centralize platforms to reduce manipulative activities.

Informed and Protected Activity. Users have different levels of experience and understanding of blockchains and the associated risks. Activity on platforms should be informed and protected due to the high risks involved with participating.

A. THE REGULATORY FRAMEWORK: THREE TIERS

1. Tier One: Known Breaches

Users must have confidence that platforms are safe and that content on platforms is accurate. To encourage such confidence, platforms need to implement certain control requirements within their operations, particularly relating to content moderation and authorization. Second, users must be aware of the risks associated with using a particular platform. To inform users, platforms need to provide users with complete and honest disclosures regarding platform performance.

Control Requirements. Platforms need to implement control requirements that authenticate the accuracy of content. First, platforms should be required to verify the authenticity of accounts. Financing users would disclose identifiable information to verify the existence and

239. Sherman Lee, *Blockchain is Critical to the Future of Data Storage—Here's Why*, FORBES (June 8, 2018), https://www.forbes.com/sites/shermanlee/2018/06/08/blockchain-is-critical-to-the-future-of-data-storage-heres-why/#5e18f96633e9 [https://perma.cc/7NUJ-UBXK].

authenticity of ICOs. Although disclosure requirements may be difficult to enforce due to the interests of self-regulating bodies to keep platforms decentralized, platform-user collaboration that is amenable to both parties may be necessary to reduce manipulative activities. In accordance with the decentralized nature of blockchains, financing users should not be required to disclose all financial information that would be required in an ICO. Instead, financing users should be required to disclose at least one legitimate contact in the company. A requirement to verify the legitimacy of an ICO can also make platforms more willing to check the content available. This requirement can make manipulative users less willing to scam users with fake ICOs.

Creation of IT Specialist Team and Performance Reports. Users should be informed of the risks involved in using a platform. Informed users may prefer to use one platform over another and may adjust the amount of money or information used on a platform when they decide to use a platform with greater risks. To be completely informed, users must be aware of platform performance and risks related to platform activity. Platforms need to provide users with performance reports with pertinent information regarding the risks associated, such as past performance statistics and the causes and consequences of risks. To accomplish this, platforms should establish monitoring systems to continuously oversee the blockchain and create a team of IT specialists to report abnormal activities and produce an objective report of platform performance.

Programmers can be instrumental in monitoring systems because they work closely and frequently with blockchains. They may be able to detect abnormal activities during the course of carrying out their ordinary tasks. However, programmers typically work with a limited type of transactions. Moreover, programmers can be mining-users who independently participate in transactions. Therefore, a new group of employed programmers—IT specialists—should deal with the overall performance of the platform. The team of IT specialists would consist of highly experienced programmers that support companies by solving technical problems. They would assess platform performance by working on ongoing and forward-looking technical problems on the blockchain. Contrary to the programmers' duties, IT specialists should not be assigned to code transactions onto the blockchain. Like auditors, IT specialists should generally remain independent. Based on these activities, IT specialists can provide authentic, objective opinions on platform performance by way of reports. Like audit reports, performance reports should be a reliable source on which users can base their participation and

investment decisions. Although this proposition generally takes after the auditing principles of securities regulation, performance reports would inform users on platform performance in regard to technology and content, including the status of platform technology, data relating to successful and unsuccessful transactions, and overall user-participation activities. Reporting standards must reflect the content and technology with regard to the intended audience. Procedures must provide guidelines for IT specialists to prepare the report and if followed, provide users with a comprehensible, accurate opinion on a platform's overall performance.

Designing the reporting standards and procedures would require expertise in blockchains and law. Blockchain experts, including lawyers, regulators, and developers could create guidelines for platforms. But this method does not yield long term improvements to blockchain technology, its services, or the industry. The industry may benefit from the oversight of an entity such as the PCAOB. A designated committee could oversee IT specialists and provide advice and direction. Platforms could bolster secure services to the public. Performance reports would have the added benefit of informing developers of the technology's progress and providing guidance on technological issues.

2. Tier Two: Suspected Breaches

Tier Two relates to measures following platforms' duty to monitor and detect abnormal activities. Users must be informed in circumstances of suspected breach and offered access to the platform's prophylactic practices in order to protect themselves before any actual breaches occur. Such users would be able to make informed, strategic steps through breach notification requirements.

Breach Notifications. Platforms need to implement breach notification requirements to inform users of suspected breaches. The breach notification requirement must address what information should be disclosed to users and when such information is to be disclosed. Given that they are not licensed specialists, like accountants and lawyers, users should be notified with extreme care.

In the event that programmers suspect abnormal activity, they should be required to report the activity up the corporate hierarchy. If programmers become aware of suspicious activity, they should first be required to report abnormalities to an IT specialist. The IT specialist should inquire further into the finding and determine whether an attack or loss has occurred—or is likely to occur. First, reporting out should not be left to the reporter's discretion. The programmer has only received

feedback from the IT specialist. Users cannot be expected to assume potential liabilities and moreover, do not have deep pockets like issuers. Second, reporting out to users must only be done after a thorough investigation and concrete analysis. Users who are notified of a suspected breach may not comprehend the issue or know how to move forward. Programmers must determine that there is a clear breach and reasonably believe that the breach is reasonably certain to result in substantial injury to users.

The requirement to report out may not be ideal where most programmers are miners. There is no way to verify whether miners are actually monitoring activity, and the miners may not be qualified to make such determinations. However, since platform activity is largely a result of miners, it may still be favorable to encourage miners to report such activity to programmers and IT specialists. Miners have incentives to report such activity since the performance relates to abnormal activities and manipulative practices.

Write-In Exceptions. In addition to the notification requirements to prevent breach, platforms should implement corrective actions, the "write-in exceptions," to protect users from ensuing harm. Write-in exceptions are lines of code in a smart contract that allow blockchain platforms to reverse transactions depending on whether a transacting party committed a material violation. After determining that there is an actual, substantial likelihood of injury, platforms should inform users of the susceptible accounts and should be ready to exercise the write-in exception in situations where the user was not able to protect the account or its value in time.

Immutability is a pivotal aspect of blockchain technology. The technology and the roles of the parties in the industry revolve around this characteristic: platforms provide services that guarantee the execution of transactions and contracts; users rely on that guarantee to participate in secure exchanges; miners help protect the integrity of blockchains by working on an honor system—the hashing system; parties continue to rely on blockchain technology, and developers and programmers are encouraged to develop the technology and its services accordingly. The continued expansion of the blockchain industry is dependent on the preservation of blockchain's immutability. Therefore, the write-in exception should be exercised only in limited circumstances of certain material violations, such as system manipulation. In addition, the reversal of transactions can initiate an uprising in misappropriated funds and wrongful ownership, and thus, must be employed with extreme care. To

protect the integrity of blockchains, write-in exceptions need a clear definition. Platforms may need to qualify IT specialists to track and remove certain users and to institute write-in exceptions to reverse transactions depending on materiality. To safeguard the write-in exception from abusive use, the write-in should be explainable if the grounds for such actions are questioned in a proceeding. In such circumstances, the platform should be protected for decisions made in good faith.

3. Tier Three: Inevitable Breaches

The third tier relates to inevitable breaches, which are breaches that are bound to happen regardless of whether platforms and users comply with tier one and two. Users around the world are increasingly relying on blockchain technology for banking and contracting needs and thus, need to be protected in the event of a blockchain fail. The regulatory framework should prioritize the protection of all parties in the blockchain industry. Although user protection is essential to the continuous growth of the blockchain industry, platforms need incentives—aside from profits—to continue experimenting to develop the technology and provide new and improved services. Given the infancy of the industry and the unpredictability of the technology in practice, platforms must engage in risky business ventures to test and develop the technology. To encourage blockchain development, regulatory development must take these inevitable aspects into consideration.

The effort to balance liability and encourage shared responsibility should be viewed in light of the general backdrop of the corporate setting: investors are free to invest in the corporation of their choice, but bear the burden of its consequences—good or bad—provided that they were given the information sufficient to make an informed decision. Once an informed investment is made, the investing party becomes an investor of a particular corporation and agrees to abide by the consequences of that corporation's past, current, and future decisions. In exchange, the investor holds rights to dispute the information that the corporation provided and to challenge the decisions made by the corporation's board of directors in a court proceeding for the resulting damages. In a court proceeding, the investors may challenge the board's decision on the basis of how that decision was made. To safeguard the corporation's board of directors from frivolous litigation brought by its investors, however, courts defer to the business judgment of corporate executives. Under the business judgment rule, the board of directors cannot be held liable for losses

incurred by investors if the losses resulted from decisions made with reasonable care.[240] This rule takes into consideration the volatility of the financial world and pardons losses that may be incurred as a result.

Similarly, any regulatory developments in the blockchain industry must take into consideration the unpredictability of the technology and volatility of its application in a platform. Along with the propositions provided in Tier One and Tier Two, the parties in the blockchain and smart contract industry should be made aware of the difficulties in attempting to develop a new technology-based industry. The nature of blockchain makes new attacks, and the resulting losses, inevitable. Additionally, parties should understand that with this inevitability come situations of no liability, where there may not be an appropriate party to attach liability. For example, users may not be able to recover losses incurred from attacks if platforms establish systems to monitor platform performance and maintain system security measures in good faith. Platforms should not be required to payroll a staff of highly qualified programmers, perform duties to protect users, and also have to reimburse for user losses. However, the loss was already incurred, and the user was already harmed. In these circumstances, protection should be available to all parties in the industry.

Cyber Insurance Policies. Even if platforms comprehensively monitor blockchains, there may be abnormal activities that are unrecognizable at first glance. Accordingly, platform companies should provide—either personally or via third-party insurers—cyber insurance policies to their users and require users to purchase cyber insurance before participating on the platform. Users should be required to purchase cyber insurance policies providing protection against damages resulting from threats to electronic data. Such policies will certainly protect users, since the threats to electronic data can result in stolen or damaged information, expensive liability, and recovery costs. In an industry with high risks involved, the significance of insurance coverage should be endorsed.

CONCLUSION

The blockchain industry and its regulatory framework remain in their infancy and accordingly, their matured forms will be established by copious methods and numerous trials due to the decentralized nature of the blockchain industry and its underlying technology. However, the

240. *See In re* Walt Disney, 906 A.2d 27 (Del. 2006).

industry should not be burdened to address new circumstances of hacks and losses. The technology is advancing, and the industry is expected to maintain—and eventually surpass—its accumulated growth and wealth. Moreover, the industry has revealed patterns that were, and continue to be, prevalent in other industries, such as information, securities, and finance.

By identifying manipulative practices and diligently balancing the regulatory framework to acquire preferable qualities of neighboring regulations—or to avoid destructive situations caused by manipulation—the blockchain industry may discover its own regulatory needs and hopefully, manage to outwit some of the manipulative games played by its participants.