OFF THE CHAIN! A GUIDE TO BLOCKCHAIN DERIVATIVES MARKETS AND THE IMPLICATIONS ON SYSTEMIC RISK

Ryan Surujnath[*]

Blockchains are publicly viewable and theoretically unalterable records of bitcoin transactions. They are thus crucial to the functionality of cryptocurrencies. Through the blockchain, bitcoin algorithmically decentralizes the maintenance of the transaction ledger and delegates the task to users on its network.

Blockchain technology shows promise beyond cryptocurrency: banking and financial institutions have established partnerships with fintech firms to explore the applicability of blockchains in capital markets. Blockchains, used in conjunction with self-executing smart-contracts, present particularly compelling opportunities in derivatives markets, which are typically beset by numerous intermediaries. The blockchain could radically reinvent the existing market infrastructure. Certain intermediaries like central counterparties could become redundant or see abbreviated functionality. If this happens, the current body of derivatives laws and regulations would need to be amended to reflect these changes.

This Note examines the blockchain's functionality and its applicability to derivatives markets. It discusses the current state of derivatives regulation, including the mandatory clearing mandate imposed by Title VII of Dodd-Frank. This Note argues that the current regulatory scheme is underpinned by a need to reduce the systemic risks posed by derivatives and that the new regulatory blueprint for blockchain derivatives markets should consequently be motivated by a reduction of the systemic risks inherent in the technology itself.

TABLE OF CONTENTS

---

* J.D. Candidate, 2017, Fordham University School of Law; B.A., 2014, Rutgers University. The author would like to thank Olivier Sylvain for taking time to discuss and develop this topic. The author also wishes to thank his family for their support and patience.

INTRODUCTION

It has been seven years since a person (or persons), writing under the pseudonym Satoshi Nakamoto, proposed a radical plan for a decentralized and completely digital currency.[1] Nakamoto's opus, published as the world's financial markets reeled from one of the worst crises in recent memory, envisioned a structure where the systems typically monopolized by sophisticated intermediaries could be crowdsourced to members on a common network.[2] Bitcoin captured the imaginations of those who yearned for a more egalitarian economy. Free from government control,

1. *See generally* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008), http://bitcoin.org/bitcoin.pdf [https://perma.cc/4CHK-MUNP]. For years, journalists have speculated on Nakamoto's true identity. Suspects have included a model train collector from Los Angeles and, most recently, an Australian computer scientist. *See* James Titcomb, *Satoshi Nakamoto, Whoever That Is, Will Not Rescue Bitcoin*, TELEGRAPH (May 8, 2016), http://www.telegraph.co.uk/technology/2016/05/08/satoshi-nakamoto-whoever-that-is-will-not-rescue-bitcoin [https://perma.cc/FE8Q-3PZ9].

2. *See generally* NAKAMOTO, *supra* note 1.

Bitcoin separated economic liberties from political ones.[3] Anyone with access to an internet connection can access Bitcoins. Yet amidst these lofty aspirations, Bitcoin suffered numerous setbacks, from wild price fluctuations[4] to the infamous Mt. Gox[5] and Silk Road[6] scandals. Many question whether Bitcoin can expand beyond a niche, tech-savvy user-base.[7] While Bitcoin is still a prominent payment system, new fintech startups are instead homing in on its underlying technology, the blockchain. Indeed, "blockchain" is somewhat of a buzzword in the finance industry these days. Since 2014, venture capital firms have invested more than $1.2 billion into blockchain startups.[8] Wall Street's traditional firms find themselves working alongside upstart fintech companies to apply the technology to today's capital markets.[9]

---

3. *See* ALEX TAPSCOTT & DON TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD 6 (2016).

4. *See* WINKLEVOSS INDEX, http://winkdex.com [https://perma.cc/MZT2-XKFC] (providing historical bitcoin pricing data). When dealing with foreign exchange rates, bitcoin is commonly abbreviated "BTC." *See id.* One of the biggest spikes in the BTC/USD exchange rate was in 2013; it began the year at 1 BTC=13.45 USD. *See id.* By early December, the exchange rate had reached its historical high, where 1 BTC roughly equaled 1140 USD. *See id.* Observers cite several reasons for the spike, including a bank bailout in Cyprus that led worried depositors to seek safe havens. *See* Maureen Farrell, *Bitcoin Prices Surge Post-Cyprus Bailout*, CNN MONEY (Mar. 28, 2013), http://money.cnn.com/2013/03/28/investing/bitcoin-cyprus [https://perma.cc/T493-TCHJ].

5. *See* Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014), http://www.wired.com/2014/03/bitcoin-exchange [https://perma.cc/2SQQ-EUGN]. Mt. Gox was the biggest Bitcoin exchange in the world until more than $460 million in digital currency disappeared from beneath management's nose. *Id.*

6. *See* Joshua Bearman & Tomer Hanuka, *The Rise & Fall of Silk Road*, WIRED (Apr. 2015), http://www.wired.com/2015/04/silk-road-1 [https://perma.cc/6EA4-NSRZ]. Bitcoin was implicated in the Silk Road affair because users paid for illicit goods using the currency. *See id.*

7. *See* Zoe Thomas, *Does Bitcoin Still Matter?*, BBC (May 6, 2016), http://www.bbc.com/news/technology-36197703 [https://perma.cc/6548-VZ5U].

8. For a list of blockchain venture capital projects, see *Blockchain Venture Capital*, COINDESK, http://www.coindesk.com/bitcoin-venture-capital [https://perma.cc/QC8T-XX7J].

9. One such venture is the Hyperledger Project, a collaborative research and development effort between tech companies and financial institutions led by the Linux

At their core, blockchains are about trust and transparency among unknown peers in the absence of mutually agreed upon intermediaries.[10] Upon first glance, it seems paradoxical that an industry that thrives on information asymmetries and market gatekeeping would be so eager to embrace the technology. However, the potential for blockchains to reduce transaction costs gives firms reason to believe that the future could hold truly "frictionless" transactions.[11] While there is great potential for blockchains to create new efficiencies, regulators must remain on top of this emergent technology. In derivatives markets, regulators are especially cognizant of systemic risks that can be transmitted across the entire economy through tangled webs of connected obligations. On one hand, blockchains can contribute to the reduction of systemic risks by crowdsourcing tasks typically conducted by large central counterparties that assume large amounts of risk.[12] At the same time, the nature of blockchain technology can create systemic risks of a completely different character.[13]

Introducing the blockchain into derivatives markets can distribute processes typically undertaken by a central counterparty ("CCP"). While this can produce efficiencies, decentralized systems are not insusceptible to exploitation by users on the network. The technology itself can serve as a source of market-wide risk. This Note argues that applying blockchains to derivatives markets requires regulators to rethink assumptions about centralization and systemic risks. Part I describes the function of blockchains, discusses the core processes in derivatives trades, and explains how blockchains can apply to the markets. Part II highlights the legal framework governing derivatives trades, focusing mainly on the central clearing mandate imposed by Title VII of Dodd-Frank. Part III argues that central clearing presents systemic risks in the form of over-centralization, and that while blockchains can mitigate these

---

foundation. *See* HYPERLEDGER, https://www.hyperledger.org [https://perma.cc/G5PV-86GB].

10. *See generally* Sarah Underwood, *Blockchain Beyond Bitcoin*, COMM. ACM, Nov. 2016, at 15.

11. *See* IBM, BLOCKCHAIN–BUILDING FRICTIONLESS ECOSYSTEMS 4 (2016).

12. *See infra* Part III.

13. *See infra* Part III.

risks to some extent, regulators must tailor any new blockchain-centric policies to the unique market-wide risks posed by the technology.

I. APPLYING BLOCKCHAINS TO DERIVATIVES MARKETS

A. BUT WHAT IS A BLOCKCHAIN, REALLY?

Those who have heard even a fraction of the industry enthusiasm might be led to believe that blockchains are elixirs to all the world's problems. In part, this is because the most ambitious blockchain visionaries consider its large-scale applications beyond finance.[14] Some even suggest that blockchains possess sufficient verification mechanisms to run entire systems of direct democracy, where citizens can securely vote from a smartphone or other connected device.[15] The suggestion is astounding, especially in a political climate where allegations of voter fraud and political hacking have become matters of national salience. How, then, can a blockchain overcome fundamental issues of trust?

Ultimately, blockchain is a development in information technology.[16] Many enterprises, whether in financial services or otherwise, need to store important information as data on a central server. Blockchains can overcome some weaknesses inherent to centralized data storage. Centralized storage provides a single point of failure that, if compromised, can harm a business. Most prominently, central servers are easy targets for malicious hackers to exploit.[17] Sometimes, companies hold sensitive consumer and employee information on central servers that

---

14. *See* Nina Kilbride, *Self-Driving Vehicles and Smart Contracts via the Blockchain*, CRYPTOCOINS NEWS (Apr. 1, 2016), https://www.cryptocoinsnews.com/self-driving-vehicles-and-smart-contracts-blockchain/ [https://perma.cc/YVD6-JLWM]. Outside of finance, blockchains show promise when use in conjunction with "Internet of Things" technology. *See id.*

15. *See generally* PHILIP BOUCHER, WHAT IF BLOCKCHAIN TECHNOLOGY REVOLUTIONISED VOTING? (2016), http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA(2016)581918_EN.pdf [https://perma.cc/RXS3-Q4NW].

16. *See* MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY (2006).

17. *See What is Blockchain Technology? A Step-by-Step Guide for Beginners*, BLOCKGEEKS, http://blockgeeks.com/guides/what-is-blockchain-technology [https://perma.cc/36AL-WWCC].

are subject to dubious data protection standards.[18] Hackers can then leak information online, forcing the affected company to incur reputational and financial costs to repair the damage.[19] Less dramatically, the system can be subject to bottlenecks or crashes if too many users access it at the same time.

In addition, a centralized system may be inefficient for organizations that must constantly modify and monitor arrangements with other parties. Consider an arrangement among a supplier, a buyer, and the bank effectuating payment. Each of these entities may need to collaborate on different aspects of the transaction. One of the hallmarks of centralized databases, however, is that only one copy of a record exists at a time. To borrow a simple, but apt, analogy by venture capitalist William Mougayar, this is the equivalent of two parties attempting to draft a contract by making revisions in Microsoft Word.[20] In comparison, blockchains are analogous to Google Docs.[21] With Google Docs, collaborating parties can grant permissions authorizing others to access or edit a document.[22]

A blockchain is a distributed ledger, where every participant on a network has the same copy of a record.[23] Blockchain networks are continually reconciled, meaning that the blockchain updates itself roughly

---

18. *See* Peter Elkind, *Inside the Hack of the Century*, FORTUNE (June 25, 2015), http://fortune.com/sony-hack-part-1 [https://perma.cc/7M74-Y6PT]. Fortune's three-part investigation delved into the infamous 2014 cyber-attack on Sony Pictures. *See id.* The attack compromised personal information of employees and embarrassing internal emails concerning ongoing movie negotiations. *See id.* While Sony maintained that its defenses were adequate, the article suggests that it failed to implement basic safeguards. *See id.* More concerning is the fact that inadequate data protection is not atypical, as experts say that "outmoded [cybersecurity] practices are the norm at far too many companies." *Id.*

19. *See, e.g.*, Ingrid Lunden, *Target Says Credit Card Data Breach Cost It $162M in 2013-14*, TECHCRUNCH (Feb. 25, 2015), https://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14 [https://perma.cc/4PPM-2HDA].

20. *See* William Mougayar, *Explaining the Blockchain via a Google Docs Analogy*, STARTUP MGMT. BLOG (Sept. 6, 2016), http://startupmanagement.org/2016/09/06/explaining-the-blockchain-via-a-google-docs-analogy [https://perma.cc/BP6Q-ZRNB].

21. *See id*.

22. *See id*.

23. *See What is Blockchain Technology*, *supra* note 17.

every ten minutes to reflect changes that occurred since the last update.[24] Because every participant on the network has an equally viable and current version of the ledger from which to work, the entire enterprise need not cease to function if a central database fails; if one participant loses its record for some reason, everyone else can keep going.[25]

The specific operation of the blockchain differs among various types—Ethereum's blockchain may differ from IBM's—but the guiding principles remain the same. The blockchain itself serves as a record of information.[26] Network participants verify the transactions by their peers, but only rightful asset holders have cryptographic keys to their accounts.[27] When an asset holder transacts on the blockchain, it proposes an amendment to the ledger, and the rest of the network verifies that the transaction is legitimate.[28] By these methods, the members of the network need not trust one another as long as they trust the computing process. To understand the details of how the process works, consider the blockchain's first and most successful application: Bitcoin.

B. BITCOINS, BLOCKCHAINS, AND SMART CONTRACTS

Initially, blockchains were not designed for use with securities, derivatives, or traditional capital markets. Instead, they were integral to the functionality of digital currencies, most notably Bitcoin.[29] By removing intermediaries from payment clearing, cryptocurrencies

---

24. *See id.*

25. *See id.*

26. *See* Casey C. Sullivan, *How Blockchain Could Improve Record Keeping*, FINDLAW (Mar. 22, 2017), http://blogs.findlaw.com/technologist/2017/03/how-block chain-could-improve-legal-record-keeping.html [https://perma.cc/62BE-EA5C]. The blockchain's record-keeping functions can have serious implications for legal professionals. *See id.*

27. *See* William Mougayar, *Understanding the Blockchain*, O'REILLY (Jan. 17, 2015), https://www.oreilly.com/ideas/understanding-the-blockchain [https://perma.cc/6 D9V-XCX2].

28. *See* NAKAMOTO, *supra* note 1, at 2.

29. Today, there are dozens of cryptocurrencies that use some variant on blockchain technology. *See, e.g.*, LITECOIN, https://litecoin.org [https://perma.cc/R76Z-BDP4]; DOGECOIN, http://dogepay.com [https://perma.cc/9XGV-HXP5].

promised to remove the main gatekeepers to sources of capital.[30] When computers solve the cryptographic puzzles, they prove the veracity of the pending transactions. The blockchains are thus integral to Bitcoin's viability.

The early stage of blockchain functionality is often referred to as "Blockchain 1.0."[31] Recently, however, finance firms have recognized the potential efficiencies they could realize if they employed blockchains outside of just cryptocurrencies. The era of "Blockchain 2.0" envisions wider acceptance of the technology across the financial sector.[32] Having seen the benefits that decentralization affords cryptocurrencies, many on Wall Street believe that blockchains can streamline existing market processes and create massive cost savings and efficiencies.[33]

To understand how blockchains work and the benefits they provide, it is useful to begin with Blockchain 1.0. While there exist many different cryptocurrencies, this Note focuses on the two most popular: Bitcoin and Ethereum. Bitcoin is the most popular cryptocurrency and the progenitor of blockchains. Thus, there is a large body of work on Bitcoin's functionality. Ethereum is the second most prevalent cryptocurrency and has become a prominent part of "Blockchain 2.0," thanks to its implementation of automated, customizable smart contracts.

1. Bitcoin's Underlying Technology

Transactions that occur in person are straightforward. One party sells an item of value, and its counterparty pays for the item in cash. The party

---

30. One of Bitcoin's earliest promises was the potential for "microfinance." *See* Bitcoinist.net, *ProudSource Puts New Spin on Bitcoin Peer-to-peer Lending*, INSIDE BITCOINS (June 5, 2016), http://insidebitcoins.com/news/proudsource-puts-new-spin-on-bitcoin-peer-to-peer-lending/32988 [https://perma.cc/T9G5-DE4A]. Because intermediaries require transacting fees, it is not profitable for traditional lending institutions to issue small loans to certain populations. By using blockchains as intermediaries instead, cryptocurrency enthusiasts suggest that peer-to-peer lending could be a possibility, though there are some obstacles. *See id.*

31. *See, e.g.*, SWAN, *supra* note 16.

32. *See id*.

33. *See* Robert Hackett, *Big Business Giants from Microsoft to J.P. Morgan Are Getting Behind Ethereum*, FORBES (Feb. 27, 2017), http://fortune.com/2017/02/28/ethereum-jpmorgan-microsoft-alliance/ [https://perma.cc/TK6H-CAJW].

receiving the cash payment can easily confirm the veracity of the transaction. Ensuring that the money exists and is in the appropriate amount is merely a matter of counting bills. Once money has been spent on something, it is, regretfully, gone for good.

Today, simple cash transactions are less commonplace than they were in the past. This is not a shocking revelation, as the Internet has displaced cash transactions for years, and credit cards have done the same for decades. What may be more surprising is the pervasiveness of asset digitization and its status as a preferred payment method. With Venmo, for example, users with a bank account or credit card can transfer electronic funds to one another with their smartphones.[34] Some European countries are even attempting to forsake cash altogether: in Denmark, a pending law would allow some merchants to reject cash payments, while Norway aims to become completely cash-free by 2020.[35]

The digitization of cash, while convenient, presents challenges regarding transaction verification. Coders call this the "double spending problem": if money amounts to ones and zeroes, what is stopping an opportunistic buyer from copying the code and sending it to multiple parties, as one would do to a common image or document file?[36] With the blockchain, Bitcoin addressed the double spending problem in a unique way: it removed the intermediaries that are usually crucial to digital spending platforms and crowdsourced the task to members of the network.[37] Though the parties on the network do not know one another and thus have no reason to trust one another, they all accept the code as the ultimate arbiter of truth. Transaction verification on the blockchain involves a communal search for the truth; once a user finds the correct values, the network universally adopts this as the true account of a transaction.[38]

---

34. *See* VENMO, https://venmo.com/about/product/ [https://perma.cc/BL67-QCK4].

35. *See Is Cash an Endangered Species?*, BNP PARIBAS (Aug. 14, 2015), https://group.bnpparibas/en/news/cash-endangered-species [https://perma.cc/7JTW-XDAB].

36. *See* TAPSCOTT & TAPSCOTT, *supra* note 3, at 10.

37. *See* Matt Reynolds, *Cash, Fear, and Uncertainty: The Holy Trinity of Bitcoin and Blockchain*, REGISTER (Apr. 12, 2016), https://www.theregister.co.uk/2016/04/12/bitcoin_blockchain/ [https://perma.cc/ZB5D-5WBH].

38. *See generally* Leslie Lamport, Robert Shostak & Marshall Pease, *The Byzantine Generals Problem*, 4 ACM TRANSACTIONS ON PROGRAMMING LANGUAGE & SYS. 382

The Bitcoin blockchain manufactures trust by creating a proof of work problem.[39] To verify a transaction, computers on the network must produce a particular set of data.[40] To do so, they solve an algorithmic problem.[41] The problem is computationally tedious; there is no mathematical "shortcut," no way to cut corners, and users must expend resources (time, computing power, hardware costs, electricity) to solve it.[42] While the problem is difficult for systems to solve, it should be easy for members on the network to check transactions against the public ledger.[43]

To understand how proof of work blockchains operate, consider the anatomy of a simple Bitcoin transaction. Suppose that Alice wants to pay Bob.[44] Both Alice and Bob have wallets on their computers, which store

---

(1982). *See also Bitcoin and the Byzantine Generals Problem*, WEUSECOINS (July 13, 2015), https://www.weusecoins.com/bitcoin-byzantine-generals-problem/ [https://perma.cc/MG59-NDVW]. In computer science lingo, the underlying issue that the blockchain aims to prevent is known as the Byzantine Generals' Problem. *See id.* Imagine the Byzantine army laying siege to a city. The city is surrounded by different Byzantine legions, each commanded by a different general. There is disagreement about the best course of action. Some generals want to attack the city, while others want to retreat. Whatever the decision, it is important that the action is universally agreed upon, since a half-hearted strategy would result in more casualties than a unified attack or retreat. The issue is complicated by traitorous generals who may strategically cast conflicting votes to maximize casualties. There are also communication difficulties, since the generals' messengers may be killed before communicating a vote. Bitcoin and other decentralized networks face this problem. *See id.* The network functions only if all parties are able to agree on the veracity of a transaction. *See id.* Any disagreements pertaining to the true state of affairs undermines confidence in the system. *See id.* The point of the code is for the network to resolve any differences in the verifying systems' "opinions" of a transaction. *See id.*

39. *See* Daniel Krawisz, *The Proof of Work Concept*, SATOSHI NAKAMOTO INST. (June 24, 2013), http://nakamotoinstitute.org/mempool/the-proof-of-work-concept/ [https://perma.cc/N2JH-K6LC]; *see also* Khan Academy, *Bitcoin–Proof of Work*, YOUTUBE (May 1, 2013), https://www.youtube.com/watch?v=9V1bipPkCTU.

40. *See* Krawisz, *supra* note 39.

41. *See id.*

42. *See id*.

43. *See id.*

44. The Alice and Bob hypothetical is commonly used to describe bitcoin transactions. *See, e.g.*, *How Do Bitcoin Transactions Work?*, COINDESK (Mar. 20, 2015), www.coindesk.com/information/how-do-bitcoin-transactions-work [https://perma.cc/JL6V-XFZU].

information pertaining to their Bitcoin addresses.[45] Visually, an address is a string of letters and numbers, but each address has its own Bitcoin balance.[46] To accept payment, Bob creates a new address.[47] Alice tells the Bitcoin client that she wants to send payment to Bob's new address.[48]

Had Alice and Bob kept traditional books and records, recording the transaction would be simple: Alice's books would record the transaction as a credit and Bob's books would contain a corresponding debit.[49] Recordation into the blockchain ledger, however, requires a third entry—a cryptographic seal.[50] To do this, Bitcoin uses public key cryptography.[51] Both Alice and Bob have addresses that they can disseminate publicly.[52] Additionally, Alice and Bob both have private keys, which are kept secret and derived from their addresses through a cryptographic sequence.[53] To facilitate payment, Bob gives Alice his address, which serves as a public key.[54] Alice then authorizes the transaction by "signing" the transfer with her private key and pairing it with Bob's public key.[55]

Once the deal is consummated, the transaction request is broadcast to the network for verification.[56] Miners are participants on the Bitcoin network who verify transactions for entry onto the blockchain.[57] Miners verify transactions by matching the private key signature to the transferor's publicly viewable address.[58] They periodically bundle

---

45. *See id.*

46. *See* BLOCKCHAIN, https://blockchain.info [https://perma.cc/3R5A-36JW]. Blockchain.info is the publicly viewable Bitcoin blockchain. Simply click on a block to see the recent transactions that compose the block. Each transaction appears to be between two random alpha-numeric strings—these are the addresses.

47. *See How Do Bitcoin Transactions Work?*, *supra* note 44.

48. *See id.*

49. *See id.*

50. *See id.*

51. *See id.*

52. *Id.*

53. *See* SWAN, *supra* note 16.

54. *See How Do Bitcoin Transactions Work?*, *supra* note 44.

55. *See id*.

56. *See id.*

57. *See id.*

58. *See* BITCOINMINING.COM, https://www.bitcoinmining.com/ [https://perma.cc/32LY-HWLF].

pending transaction data into blocks.[59] At that point, the miners' computers must solve the proof of work problem to essentially convert the raw transaction data into a form that is useful for systems accessing the blockchain.[60]

The proof of work problem requires miners to undergo a process called cryptographic hashing.[61] Hashing is an integral concept behind blockchain.[62] Any data set can be run through a hashing algorithm that produces a hash value, a unique alphanumeric string.[63] Even small changes to the input data can produce radically different hashes.[64] There is no way for a user to predict what hash a data set may produce without running it through the algorithm.[65] Ultimately, miners want to produce a hash that is beneath a certain target value set by the network.[66] The blockchain determines the target value to adjust the difficulty of the proof of work problem.[67] As more miners participate in the transaction verification process, the total processing power on the network increases.[68] The Bitcoin chain adjusts the target value to reflect these changes; by creating a lower target value, the blockchain decreases the number of viable solutions to a proof of work problem, making it more difficult.[69] To solve the proof of work problem, miners will use three pieces of data as inputs for the hashing algorithm: the transaction block they just formed, the hash from the previous block on the blockchain, and

---

59. *See id.*

60. *See id.*

61. *The Disruptor Series: Digital Currency and Blockchain Technology: Hearing Before the Subcomm. of Commerce, Manufacturing & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. 47 (2016) (testimony by Paul Snow, Chief Architect and Co-Founder, Fatcom, Inc.).

62. *Id.*

63. *See id*.

64. *See id.*

65. *See id.*

66. The target value sets the difficulty of the proof of work problem. The fewer acceptable values there are, the harder it is to solve the problem. Bitcoin does this because it wants to limit how many Bitcoins are in circulation. *See FAQ*, BITCOIN, https://bitcoin.org/en/faq [https://perma.cc/LZ3M-TQ7Z]; *see also* Krawisz, *supra* note 39.

67. *See* BITCOINMINING.COM, *supra* note 58.

68. *See id.*

69. *See id.*

an arbitrary number called a nonce.[70] A nonce is a variable, while the other inputs are constants. By changing the nonce, miners can produce different hash values even if the other input data remains the same.[71]

At this point, the grunt work begins. Miners will expend resources to find a nonce that will produce a hash that is beneath the target value.[72] They compete against one another in this endeavor, motivated by the promise of a Bitcoin bounty to the first miner to find an acceptable hash. The process is computationally tedious.[73] It is akin to plugging in values for variables in algebraic equations until happening upon the correct solution.[74] Unlike simple algebra, however, there is no formula or shortcut that simply "solves for *x*." The only way for miners to get an edge over the others is to purchase specialized hardware or mine in collective pools to increase the rate at which their systems run through the hashing algorithm.[75] While this helps, stumbling upon the correct hash value is still a matter of probability.[76]

When a miner finds the solution to the proof of work problem, it broadcasts the completed block to all the nodes on the network.[77] Nodes are connected systems that accept blocks by checking them against the network's acceptance criteria; if the block shows a double-spent coin, for example, the node will reject the block.[78] A node accepts a block by using the hash value of the completed block as the header for the next block in the chain.[79] Nodes always accept the longest chain of blocks to be the network's "truth."[80] If a node receives conflicting blocks, it will begin

---

70. *See id*.

71. *See id*.

72. *See* Krawisz, *supra* note 39.

73. *See* BITCOINMINING.COM, *supra* note 58.

74. *See* Krawisz, *supra* note 39.

75. *See Bitcoin Mining Hardware Guide*, BITCOINMINING.COM, https://www.bitcoinmining.com/bitcoin-mining-hardware/ [https://perma.cc/F35A-46YE]. Today, most mining occurs by collective pools rather than individuals. *See* Jordan Tuwiner, *Bitcoin Mining Pools*, BITCOIN WORLDWIDE (Mar. 25, 2017), https://bitcoinworldwide.com/mining/pools/ [https://perma.cc/J7CE-28RZ].

76. *See* BITCOINMINING.COM, *supra* note 58.

77. *See* NAKAMOTO, *supra* note 1, at 3.

78. *See id*.; *see also, e.g.*, *Bitcoin Core*, BITCOIN, https://bitcoin.org/en/bitcoin-core/ [https://perma.cc/6AKC-VGCK].

79. *See* Krawisz, *supra* note 39.

80. NAKAMOTO, *supra* note 1, at 3.

working on the one it receives first.[81] It saves the conflicting block, as other nodes also begin work on whichever one they receive first.[82] The node will switch to the block that becomes longer and more widely accepted.[83]

There are variations to this formula, but the proof of work mechanism was the initial model posed by Nakamoto and is still employed by Bitcoin. Most blockchains operate on some derivation of this formula, and the Bitcoin blockchain demonstrates the basic precepts of communal payment verification.

2. From Cash to Securities: Smart Contracts

Smart contracts are crucial in guiding the transition from Blockchain 1.0 to Blockchain 2.0. The term "smart contract" is a nebulous concept. As it is somewhat of a marketing buzzword, it is often used as a catch-all term to describe a host of online activity.[84] Lawyer and computer programmer Nick Szabo first defined the term in 1994. Szabo described a smart contract as:

> [A] computerized transaction protocol that executes the terms of a contract. The general objectives . . . are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.[85]

Much of the ambiguity surrounding smart contracts stems from the interplay between the traditional legal understanding of contracts and the

---

81. *Id.*

82. *Id.*

83. *Id.*

84. *See* Florian Glatz, *What Are Smart Contracts?*, MEDIUM (Dec. 11, 2014), https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad [https://perma.cc/6X2X-8ZZR].

85. TAPSCOTT & TAPSCOTT, *supra* note 3, at 56 (citing NICK SZABO, THE IDEA OF SMART CONTRACTS (1997), http://szabo.best.vwh.net/smart_contracts_idea.html [https://perma.cc/V6AZ-7V8W]).

"smart" aspect of the code.[86] Many online activities are governed by code and are legally relevant but lack the legal elements of contract formation.[87]

Smart contracts rest on the idea that the code can enforce and execute the terms of the agreement. A smart contract is "self-enforcing" if the software executes the terms without additional input from the parties.[88] This allows an arrangement to occur even in the absence of trust.[89] For example, Szabo considered a simple smart contract governing a car loan.[90] The loan's terms are expressed in code and programmed into the car.[91] The contract no longer hinges on the debtor's willingness to abide by its terms; if the debtor has the means to do so, the software ensures that he or she makes the payments.[92] If the debtor cannot make the payments, the smart contract invokes a lien by revoking the debtor's permission to start the ignition.[93] This hypothetical loan also highlights the smart contract's cost saving benefits. The bank does not need to devote manpower to constantly monitor the status of each loan and handle the paperwork required to invoke a traditional lien. It does not need to hire a debt collector, nor does it need to contend with the possibility that an unscrupulous repo man may expose it to additional liability.

Szabo's ideas were ahead of their time in the mid-1990s (though perhaps somewhat prophetic of today's era of driverless cars). Most smart contracts, to this point, have not demonstrated quite the same ability to process inputs as Szabo envisioned. Their most common use has been in multimedia digital rights management ("DRM").[94] Purchasing or renting

86. Riikka Koulu, *Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement*, 13 SCRIPTED 40, 41 (2016).

87. *See* Glatz, *supra* note 84.

88. *See* Koulu, *supra* note 86, at 54.

89. *See id.*

90. *See* TAPSCOTT & TAPSCOTT, *supra* note 3, at 56.

91. *See id.*

92. *See* Koulu, *supra* note 86, at 47.

93. *See* SZABO, *supra* note 85. Of course, Szabo recognized some of the potential drawbacks of this specific arrangement. It would, for example, be inconvenient if the bank decided to seize its collateral this way while the debtor was driving on the thruway. *Id.*

94. *See* Glatz, *supra* note 84; *see also Lex Disturbia: The Impact of Smart Contracts on the Law*, GOWLING WLG (Mar. 16, 2016), https://gowlingwlg.com/en/canada/insights-resources/lex-disturbia-the-impact-of-smart-contracts-on-the-law [https://perma.cc/66G

content on iTunes or a comparable service amounts to acquiring a limited use license. For example, users can view rental content only over a limited period, they can access music only on a certain number of compliant devices, and they can burn audio playlists to CDs only a few times.[95]

DRM arrangements achieve results without assuming monitoring and enforcement costs by making it impossible for users to violate the smart contract. Each song contains software that serves as the agreement's monitoring mechanism.[96] A movie rental, for example, is time stamped when the user begins watching it. After twenty-four hours, the software revokes the user's ability to access the video.[97] Yet DRM smart contracts are limited in their abilities. Unlike Szabo's utopian agreements, iTunes DRM does not process inputs and cannot apply the contract's terms.[98] It thus has restricted functionality. Unlike simplistic DRM, smart contracts going forward can use the blockchain's computational power and allocate the underlying assets once the agreement's conditions are calculated and satisfied.

Smart contracts uploaded to blockchains are programmed in code that embodies the "terms" of the agreement. In a way, the coded language of a smart contract is less obtuse than that of its written counterpart. To laypersons, traditional contracts evoke images of dense text walls, impenetrable legalese, and linguistic butchery designed to mitigate liability. But smart contracts reduce each term to its basic component in

---

G-VMTY]; Jeffrey Glazer, *Smart Contracts Are a Future*, U. WIS. L. SCH. L. & ENTREPRENEURSHIP CLINIC BLOG (Sept. 14, 2015), https://www.uwle.org/blog/smart-contracts-are-a-future [https://perma.cc/S8DF-75DJ]; Dean Walsh, *A Beginner's Guide to Smart Contracts*, CRYPTORIALS (Mar. 10, 2015), http://cryptorials.io/a-beginners-guide-to-smart-contracts/ [https://perma.cc/KXF6-CQAM]. iTunes, Netflix, and other content providers serve as distributors, taking a portion of revenue from media sales in exchange for managing digital rights. Blockchain smart contracts are being used to allow creators to distribute and monetize content while managing digital rights. *See* Joseph Young, *SingularDTV: A Decentralized "Netflix" on Ethereum*, BITCOIN MAG. (Sept. 1, 2016), https://bitcoinmagazine.com/articles/singulardtv-a-decentralized-netflix-on-ethereum-1472760808/ [https://perma.cc/GTL8-NKMC].

95. *See Apple Media Services Terms and Conditions*, APPLE, http://www.apple.com/legal/internet-services/itunes/us/terms.html [https://perma.cc/PEV8-N5EL].

96. *See* Glazer, *supra* note 94.

97. *See Apple Media Services Terms and Conditions*, *supra* note 95.

98. *See* Dean Walsh, *supra* note 94.

the form of "if/then" statements.[99] For all their programming complexity, it may be best to think of smart contracts as conditional payments.[100]

The process by which a smart contract is uploaded to the blockchain varies across the different types of blockchains. Because smart contracts are customizable and can be used for a variety of purposes, it is advantageous to use a blockchain that supports a wide range of programming languages. Bitcoin's chief competitor, Ethereum, was specifically designed for smart contracts, and thus permits users more freedom in drafting their programs.[101]

The process of uploading a smart contract to the Ethereum blockchain is not dissimilar from the Bitcoin transacting process discussed earlier.[102] The user does so through a transaction containing the smart contract's code.[103] This special transaction does not go to the counterparty's address, as with a normal Bitcoin transaction.[104] Instead, nodes on the network recognize the smart contract and create a special address for it.[105] The parties can later trigger the contract by sending a transaction request to the smart contract's address that fulfills the conditions necessary for the contract's execution.[106] Triggering a smart contract can result in a chain reaction: it can automatically lead to another transaction request, which may trigger another smart contract, and the process can theoretically repeat itself an infinite number of times.[107] This means that satisfying a single condition can trigger a series of smart contracts that are contingent on that obligation.

There must then be a way for the blockchain to monitor these triggering conditions. The blockchain, however, cannot keep track of every parameter that can influence the activation of a contract. Multi-

---

99. *See* Christopher Burniske, *Bitcoin and Ethereum: How Smart Contracts Work*, ARK INV. (May 29, 2016), https://ark-invest.com/research/smart-contracts-work [https://perma.cc/2M6L-NRW6].

100. *See About SmartContract.com*, SMARTCONTRACT, http://about.smartcontract.com [https://perma.cc/U5YD-94HK].

101. *See* Burniske, *supra* note 99.

102. *See About SmartContract.com*, *supra* note 100.

103. *See id.*

104. *See* Burniske, *supra* note 99.

105. *See About SmartContract.com*, *supra* note 100.

106. *See* Burniske, *supra* note 99.

107. *See About SmartContract.com*, *supra* note 100.

signatures and oracles resolve this problem by keeping track of information off the blockchain and providing a trusted signature once a condition to the contract is satisfied.

As the name suggests, multi-signature (or multi-sig) allows for more than two parties to enter into an agreement. With a "2-of-3" contract, there are three parties to the agreement and the contract requires two parties to sign with their private keys.[108] This can create escrows by allowing buyers to commit money to sellers and to third parties. If the parties consummate the transaction without issue, the buyer and seller sign the agreement, and the payment goes through. In the event of a dispute, the third party can arbitrate the dispute and release the funds.[109]

Oracles use multi-sig to incorporate outside information into the blockchain. An oracle serves as an additional signatory that attests to information that is not tracked by the blockchain.[110] It can reference an agreed upon data source and serve as an additional signature to a transaction that is contingent on a real-world event.[111] Once the required condition is met, the oracle signs the transaction with its private key to effectuate the transaction.[112] In a trading system that relies on numerous ledgers to keep track of different assets, the oracle can facilitate a payment that is contingent on a factor tracked by another blockchain.

Smart contract technology is still very much in its early stages of development, so some of the advantages and disadvantages may not be clear yet. But even as of now, the technology is compelling enough to attract significant investment.

---

108. The typical notation used to describe multi-sig arrangement is an "X-of-Y" contract where Y is the number of parties and X is the number of signatures needed to authorize the transaction. *See* Ben Davenport, *What Is Multisig, and What Can It Do?*, COINCENTER (Jan. 1, 2015), https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do [https://perma.cc/4W5Y-422X].

109. *See id.*

110. *See* Vitalik Buterin, *Ethereum and Oracles*, ETHEREUM BLOG (July 22, 2014), https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/ [https://perma.cc/9T9T-QXFN].

111. *See id.*

112. *See About SmartContract.com*, *supra* note 100.

C. THE MODERN DERIVATIVES INDUSTRY

While blockchains and smart contracts are at the cutting edge of finance, derivatives have existed for centuries.[113] Some of the earliest credit derivatives date back to twelfth century Venice, when concerned financiers sought insurance against the possibility that overseas trading ships would get lost at sea.[114] For most of recorded history, derivatives have been used as hedging mechanisms in commodities industries.[115] Contemporary derivatives agreements play an important role in the hedging strategies of banks and other financial institutions. Derivatives markets could be at the precipice of a major change, but there are risks inherent in the use of such instruments.

There are several general types of derivatives. Forward agreements specify later delivery of a quantity of assets at an agreed upon price.[116] Futures are standardized forwards that are traded on an exchange.[117] Options give the holder a right, though not an obligation, to purchase the underlying asset at a specified price.[118] Swaps involve exchanges of cash flows based on a notional amount named in the agreement.[119] Some complex instruments may involve a combination of the different archetypes.

Derivatives trades can occur either through exchanges or over-the-counter ("OTC").[120] Exchange-traded derivatives must be highly standardized and liquid.[121] Parties to these agreements have fewer choices regarding underlying assets, settlement amounts, maturity dates, and

---

113. *See* Michael Chui, *Derivatives Markets, Products, and Participants*, *in* IFC BULLETIN NO. 35: DATA REQUIREMENTS FOR MONITORING DERIVATIVE TRANSACTIONS 3, 4 (2012), http://www.bis.org/ifc/publ/ifcb35.pdf [https://perma.cc/HQ3U-7RU8].

114. *See id.*

115. *See id.*

116. *Id*. at 5.

117. *Id*.

118. *Id.*

119. *Id*.

120. *See* DEUTSCHE BÖRSE GRP., THE GLOBAL DERIVATIVES MARKET: AN INTRODUCTION 10 (2008), http://deutsche-boerse.com/blob/2532338/10c3a059fd54aa0b7a9bee49c470555d/data/the-global-derivatives-market-0508_en.pdf [https://perma.cc/ZUL6-FBL4].

121. *See id.*

other contractual terms.[122] Centralized entities can provide credit support to ensure execution of the contract and can monitor trading practices.[123] Conversely, OTC derivatives are individually negotiated. They are often bespoke and designed to deal with very specific types of risks.[124] Their terms are variable and consequently allow for limitless speculative or hedging potential.[125] However, the specificity of these contracts often makes them illiquid.[126]

1. Risks Associated with Derivatives Use

Regardless of their type, a fundamental characteristic of derivatives is long-term risk.[127] Regulators often say that they want to curtail risky practices, but this is a vague proposition when dealing with parties that quite literally trade in risk. A well-functioning derivatives market is thus concerned with mitigating unwanted risks.[128] Counterparty risk, i.e., the risk that a counterparty will be unable to fulfill its end of the contract, is the greatest source of concern for market participants.[129] As a form of credit risk, it measures the degree of exposure a firm has to the potential default of its counterparty.[130] As counterparty risk is an inherent part of every derivative transaction, it is more difficult to hedge.[131] Market participants fear a domino effect in which the default of one counterparty results in defaults of others.[132] Because firms will always assume some degree of counterparty risk in every trade, they tend to offset the risk by entering into cancelling transactions.[133] An unexpected default by a

122. *See* Sean Griffith, *Substituted Compliance and Systemic Risk: How to Make a Global Market in Derivatives Regulation*, 98 MINN. L. REV. 1291, 1297 (2014).

123. *See id*.

124. *See* Zachary J. Gubler, *The Financial Innovation Process: Theory and Application*, 36 DEL. J. CORP. L. 55, 85 (2011).

125. *See* Griffith, *supra* note 122, at 1298.

126. *See* DEUTSCHE BÖRSE GROUP, *supra* note 120, at 12.

127. *See id.*

128. *See id.*

129. *See* Gubler, *supra* note 124, at 60.

130. *See* RAFFAELE SCALCIONE, THE DERIVATIVES REVOLUTION: A TRAPPED INNOVATION AND A BLUEPRINT FOR REGULATORY REFORM 72 (2011).

131. *See id*.

132. *See id*.

133. *See id*.

counterparty to whom a firm is significantly exposed can cause previously neutralized risks to re-expose themselves.[134] That is to say, a counterparty's default can upset the firm's balanced position, causing a scenario where it must re-hedge the affected positions. If the whole market is suffering from extreme conditions, it may be impossible, or at least more expensive, to hedge.

2. The Derivative Value Chain

The value chain of a derivative can be divided into three general stages: pre-trading, trading and clearing, and execution and delivery.[135] Pre-trading involves originating and channeling orders to marketplaces.[136] During trading, buyers and sellers are matched with one another.[137] Compatible counterparties may then execute the trade by entering into the derivatives contract.[138] At this stage, the contracts are "open;" during the clearing process, open contracts can be managed and traded again throughout their maturity.[139] In modern derivatives markets, the post-trading management of the contracts is typically handled by a CCP.[140] Finally, once the agreement reaches maturity, the contract is "closed" either through a cash payment (which occurs in the majority of cases) or through physical delivery of the underlying asset.[141]

Pre-trading begins with broker-dealers.[142] In exchange-traded deals they originate orders from their customers and wire those orders to centralized exchanges called designated contract markets.[143] These designated contract markets include platforms like the Chicago Board of Trade or the New York Mercantile Exchange.[144] Typically, with these

---

134. *See id*.
135. DEUTSCHE BÖRSE GROUP, *supra* note 120, at 15.
136. *See id*.
137. *See id.*
138. *See id*.
139. *See id*.
140. *See id.*
141. *See id*.
142. *See id.*
143. *See* 7 U.S.C. § 7 (2012).
144. *See Trading Organizations–Designated Contract Markets*, U.S. COMMODITY FUTURES TRADING COMM'N, http://sirt.cftc.gov/SIRT/SIRT.aspx?Topic=TradingOrgani

standard agreements, the only negotiable terms are the price terms in futures or options contracts and the cash delivery amounts in swaps.[145] Standardization makes these derivatives highly liquid,[146] so the exchange generally has little difficulty in finding two parties that are willing to assume different sides of the transaction.

In OTC markets, broker-dealers send the orders to their own derivatives desks or, if necessary, to other dealers.[147] For swap agreements, however, the orders are sent to swap execution facilities, which provide similar pre-trade bid and ask information as the exchanges.[148] Trading is bilateral; the terms may either resemble standardized agreements ("look-alikes") or be specific to each party's needs.[149] In the latter scenario, the contract could be too illiquid for there to be a robust secondary market.

Once the parties are matched and a trade is pending, CCPs clear the trade. CCPs are organizations that consist of member firms which attempt to reduce the impact of a default on derivative contract obligations.[150] The CCP clears transactions by serving as the "buyer to every seller and the seller to every buyer."[151] The CCP inserts itself between both parties through a process called novation in which the two counterparties contract with the CCP instead of directly with one another.[152] This creates two contracts: one between the first counterparty and the CCP, and an offsetting one between the CCP and the second counterparty.[153] The counterparties are thus not exposed to each other's credit risk and are only concerned with the credit risk of the CCP.

---

zations&implicit=true&type=DCM&CustomColumnDisplay=TTTTTTTT [https://perma.cc/WP5L-TN5S].

145. *See* Thomas E. Lynch, *Derivatives: A Twenty First Century Understanding*, 43 LOY. U. CHI. L.J. 1, 11 (2011).

146. *See id.*

147. *See* DEUTSCHE BÖRSE GROUP, *supra* note 120, at 15.

148. *See* 7 U.S.C. § 7b-3 (2012).

149. *See* DEUTSCHE BÖRSE GROUP, *supra* note 120, at 16.

150. *See* AMANDEEP REHLON & DAN NIXON, CENTRAL COUNTERPARTIES: WHAT ARE THEY, WHY DO THEY MATTER AND HOW DOES THE BANK SUPERVISE THEM? 1-2 (2013), http://www.bankofengland.co.uk/publications/Pages/quarterlybulletin/2013/m13prerelease.aspx [https://perma.cc/8TQC-LS2Y].

151. Griffith, *supra* note 122, at 1312.

152. *See* REHLON & NIXON, *supra* note 150, at 4.

153. *See* Lynch, *supra* note 145, at 22.

Because the CCP absorbs all the counterparty risks on the market, it must guard against its own default through netting and collateralization.[154] Netting reduces the number of times cash changes hands.[155] When two parties have several outstanding derivatives contracts with one another, there will be some winning deals and some losing deals.[156] Rather than paying out each agreement individually, netting allows a party to subtract its losses from its gains and pay the net result.[157] CCPs engage in multilateral netting, which leads to movement consolidation among several clearing members.[158] Additionally, when a clearing member first enters the transaction, the CCP collects an initial margin as a form of collateral.[159] The requested margin reflects the probability of the member's default.[160] For example, NASDAQ's margining model for commodities derivatives reflects a 99.2% probability that the margin will be sufficient to cover a default.[161] CCPs also collect another type of margin called variation margin to adjust a position through the life of the trade.[162] Variation margins can result in a transfer of funds from the member organization to the CCP (or vice versa), depending on the change in the instrument's market value.[163] The combination of these requirements protects CCPs from both future and day-to-day losses.

D. BLOCKCHAIN'S DISRUPTIVE POTENTIAL

The derivatives industry is highly intermediated, and blockchain computation provides an opportunity for cost reductions and increased efficiencies. Goldman Sachs estimates that implementing blockchains in markets for cash securities can result in $11 billion to $12 billion in annual

154. *See id.*
155. *See id.*
156. *See* Gubler, *supra* note 124, at 90.
157. *See id*.
158. *See* REHLON & NIXON, *supra* note 150, at 3-4.
159. *See* Griffith, *supra* note 122, at 1302.
160. *See* REHLON & NIXON, *supra* note 150, at 5.
161. *See Margining Methodology*, NASDAQ, http://business.nasdaq.com/trade/clearing/nasdaq-clearing/risk-management/margining-methodology [https://perma.cc/ATZ2-5QQD].
162. *See* REHLON & NIXON, *supra* note 150, at 5.
163. *See id.*

savings to the banking industry, with additional savings if they were applied to derivatives markets.[164] Banks could see similar reductions in costs of anti-money laundering and know-your-customer reporting.[165] There have already been small-scale test cases involving successful transfers of foreign exchange futures and credit-default swaps using blockchains.[166]

A blockchain-based derivatives contract market would likely involve a system of several interoperable ledgers that use multi-sig smart contracts for effectuating transfers and oracles for asset monitoring and collateral management.[167] Parties to a blockchain derivatives transaction would submit bids and asks as usual. In OTC markets, dealers could play a reduced role. Rather than relying on the dealers to match bids and asks, parties could take advantage of the anonymity provided by the blockchain, in the same way Bitcoin users do.[168] They could upload asks directly to the blockchain and rely on its computing to automatically choose the highest bid.[169] Because of public-key cryptography, the publicly viewable addresses would serve as aliases that conceal identifying information of the counterparties.

Once the parties are matched, CCPs would novate the agreements.[170] As with the current novation process, this would result in two contracts. The contracts are then uploaded to the derivatives ledger, which contains the logic and execution algorithms for all the clearing members' agreements.[171] Posting margin to the CCP involves the use of

---

164. *See* THE GOLDMAN SACHS GRP., PROFILES IN INNOVATION: BLOCKCHAIN: PUTTING THEORY INTO PRACTICE 3 (2016).

165. *See* MCKINSEY & CO., BEYOND THE HYPE: BLOCKCHAINS IN CAPITAL MARKETS 3 (2015).

166. *See* Arjun Kharpal, *Barclays Used Blockchain Tech to Trade Derivatives*, CNBC (Apr. 19, 2016), http://www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-trade-derivatives.html [https://perma.cc/7U8Q-2AER].

167. *See generally* ISDA, THE FUTURE OF DERIVATIVES PROCESSING AND MARKET INFRASTRUCTURE 23 (2016); OLIVER WYMAN, BLOCKCHAIN IN CAPITAL MARKETS: THE PRIZE AND THE JOURNEY (2016) (describing one model of an ideal derivatives blockchain).

168. *See* WYMAN, *supra* note 167, at 15.

169. *Id.* at 11.

170. *Id.* at 10.

171. *Id.*

interoperable collateral and asset ledgers.[172] Throughout the lifespan of the agreement, the collateral ledger uses oracles to reference agreed upon external data sources (like Bloomberg) to track price movements in the underlying assets and to automatically adjust positions.[173] Rebalancing happens according to real time fluctuations, which means that collateral in margin accounts can be allocated more efficiently.[174] Execution of the payments is automated; if additional margin is needed, the ledger automatically sends a payment request to the clearing member's address on the asset ledger.

There is some disagreement among industry stakeholders as to the degree to which blockchains can displace CCPs as intermediaries in derivatives trades. The blockchain's verification mechanism threatens to eliminate CCPs in securities transactions. Blockchains ensure that both parties own the asset before the trade is consummated—this would work in largely the same way that a Bitcoin transaction works and can reduce counterparty risk without the presence of a CCP. But unlike with securities, there can be a substantial amount of time between the trade and settlement of a derivative.[175] Verifying the trade does not eliminate counterparty risk ten years down the road.[176] For this reason, many observers believe that CCPs will still be necessary to perform netting; if the blockchain is unable to net transactions, it could lead to higher collateral requirements across the board.[177] Thus, there is some skepticism that market participants and regulators will abandon the tried and true

---

172. *Id.*

173. *See* Matt O'Brien, *Blockchain Technology Will Profoundly Change the Derivatives Industry*, BITCOIN MAG. (May 27, 2016), https://bitcoinmagazine.com/articles/blockchain-technology-will-profoundly-change-the-derivatives-industry-1464368431 [https://perma.cc/WPJ5-ZZZ3].

174. *See* COMMODITIES FUTURES TRADING COMM'N, PRESS RELEASE NO. 7324-16, TECHNOLOGY ADVISORY COMMITTEE MEETING 208 (2016), http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/tac_022316_transcript.pdf [https://perma.cc/UMG9-DGEU].

175. WYMAN, *supra* note 167, at 10.

176. *See* German Banking Indus. Comm., *Response to ESMA Discussion Paper on the Distributed Ledger Technology Applied to Securities Markets*, https://www.esma.europa.eu/file/19543/download?token=g3KSQoB2 [https://perma.cc/W6ZE-5DC2].

177. *See* Euroclear Inc., *Response to ESMA Discussion Paper on the Distributed Ledger Technology Applied to Securities Markets*, https://www.esma.europa.eu/file/19531/download?token=kz0cZ0E2 [https://perma.cc/ZV5G-QXUS].

"safety net" that CCPs provide.[178] Some are more hawkish on the blockchain's displacement potential.

On the other hand, blockchain optimists suggest that an improvised netting process can occur on the blockchain. For example, in a comment to the European Securities Market Authority, the International Swaps and Derivatives Association ("ISDA") suggested that blockchains can consolidate trading information over a given period into a single aggregate movement.[179] The blockchain can then lock margin accounts until they are funded appropriately.[180] Some go a step further and suggest that the simplified settlement process sufficiently reduces counterparty risk, which makes netting unnecessary.[181] This question will be resolved as the technology matures. Since CCPs provide clear benefits, blockchains must demonstrate clear efficiencies to displace the current system.

Even if CCPs retain their functionality, blockchains still provide efficiencies by serving as platforms for data recording and reporting. Audits and other regulatory reporting become a pittance—and a potential boon for regulators.[182] By serving as a full node on the blockchain, the concerned regulator would have a copy of the entire ledger, which includes information pertaining to every transaction, margin amounts, and the risk profiles of the participating firms. There needs to be some tinkering, though: regulators would require modified permissions or an identification system to de-anonymize the accounts on the blockchain, and key management, in general, would require great care.[183] Furthermore, authorized parties have access to the smart contracts, which

178. *See* THE GOLDMAN SACHS GRP., *supra* note 164, at 52.

179. *See* ISDA, *Response to ESMA Discussion Paper on the Distributed Ledger Technology Applied to Securities Markets*, https://www.esma.europa.eu/file/19542/download?token=JfoBw0IT [https://perma.cc/7FLX-VLU3].

180. *See id*.

181. *See, e.g.*, Joe Parsons, *Blockchain Startup Aims to Replace Clearing Houses*, TRADE (Oct. 11, 2016), http://www.thetradenews.com/Technology/Blockchain-startup-aims-to-replace-clearing-houses/ [https://perma.cc/WQE3-F2DY] (describing a new blockchain startup that aims to remove clearinghouses from derivatives trades).

182. *See* Cliff Moyce, *How Blockchain Can Revolutionize Regulatory Compliance*, CORP. COMPLIANCE INSIGHTS (Apr. 9, 2017), http://www.corporatecomplianceinsights.com/blockchain-regulatory-compliance/ [https://perma.cc/A86H-LSZY].

183. WYMAN, *supra* note 167, at 15.

serve as records of ownership and vital transaction information.[184] The self-executing smart contracts can also eliminate the need for some dispute resolution procedures.[185] The blockchain's automation can yield reductions in transaction costs that firms usually incur when resolving contract disputes.

The greatest potential for blockchains likely exists in markets where there is no CCP: illiquid, non-cleared OTC derivatives markets.[186] In these markets, blockchains can assume functions typically undertaken by CCPs. But rather than relying on a single *central* counterparty, the blockchain serves as a *de*centralized clearing network ("DCN").[187] Firms trading these derivatives could use a blockchain like Ethereum, which allows users to organize into distributed autonomous organizations ("DAO") governed by smart contracts.[188] Once the criteria for admission into the DCN are met, the blockchain manages the functions usually conducted by the CCP: valuing contracts, calculating initial and variation margins, facilitating custody of collateral, handling novation and netting, and managing closeout.[189] Derivatives are contracts that have calculable terms with an "algorithm" expressed through legal terms.[190] Valuation typically presents a problem in bilateral markets because the two parties compute the algorithms themselves and may reach different conclusions on pricing.[191] Blockchains crowdsource the calculations and allow the network to reach a consensus on their accuracy.[192] Proponents hope that the communal process can result in more transparent OTC markets.[193]

---

184. *See* MCKINSEY & CO., *supra* note 165, at 9.

185. *See id*. at 1, 8.

186. *See* Ian Rycott, *What Every Trader Needs to Know About Blockchain*, FI-DESK (Sept. 22, 2015), http://www.fi-desk.com/derivatives-blockchain/ [https://perma.cc/B57K-QKFM].

187. *See* COMMODITIES FUTURES TRADING COMM'N, *supra* note 174, at 194-95.

188. *See Distributed Autonomous Organization*, ETHEREUM, https://www.ethereum.org/dao [https://perma.cc/QW9C-TW48].

189. *See* COMMODITIES FUTURES TRADING COMM'N, *supra* note 174, at 195-96.

190. *See id*. at 196.

191. *See id*. at 196-97.

192. *See id*. at 197.

193. *See* William Shaw, *EU Regulator Pushes for Transparency on Nonequity Options*, LAW360 (Oct. 3, 2016), https://www.law360.com/articles/847315/eu-regulator-pushes-for-transparency-on-nonequity-options [https://perma.cc/X7E7-LBA2].

Despite their potential to realize new efficiencies, blockchains face barriers to implementation. A system that is completely reliant on the blockchain cannot guarantee payments if there is a flaw in contracting.[194] One major drawback is the lack of legal recourse for aggrieved parties.[195] Irrevocability is a central tenet to the blockchain.[196] It should be impossible for a single entity to "edit" an entry to the blockchain and reverse it as if it never happened.[197] This can present a problem when attempting to enact a court-ordered remedy.[198] While the smart contract will undoubtedly resolve some disputes, others will remain. A smart contract does little to remedy insider trading, and new disputes could arise if a party believes that the coded logic does not accurately reflect the agreed upon terms.[199]

II. CURRENT LEGAL REGIMES GOVERNING BLOCKCHAINS AND DERIVATIVES

A. THE CURRENT LEGAL LANDSCAPE ON BLOCKCHAINS

Blockchain is still in its formative stages, and global regulators are still attempting to keep pace with fintech research in the private sector. The regulators' roles in the new, decentralized future are still far from clear, so many foreign jurisdictions have adopted a "wait and see" approach to blockchain regulation. In these countries, financial regulators are wary of impeding blockchain's technological development and instead work with industry stakeholders to ascertain the technology's capabilities.

The United Kingdom Financial Conduct Authority ("FCA") has adopted a particularly novel approach to blockchain regulation. The FCA has created "regulatory sandboxes" where "businesses [can] test

194. *See* COMMODITIES FUTURES TRADING COMM'N, *supra* note 174, at 198.

195. *See* MCKINSEY & CO., *supra* note 165, at 11.

196. *See* Josh Stark, *The Two Topics in Law and Blockchain*, COINDESK (Jan. 14, 2017), http://www.coindesk.com/the-two-topics-in-law-blockchain/ [https://perma.cc/8923-RCXE].

197. *See id.*

198. *See id.*

199. *See id.*

innovative products, . . . business models and delivery mechanisms."[200] These sandboxes serve as closed environments where startups can test blockchain use without subjecting themselves to the entire suite of U.K. financial regulation.[201] Rather than forcing blockchain startups to assume significant time and monetary costs to test new concepts in an uncertain regulatory environment, the FCA has established an abbreviated process through which approved entities can experiment with blockchains without suffering the full repercussions of failure.

The FCA has determined several requirements for admission into the sandbox. An applicant firm must be within the scope of the sandbox's objectives, demonstrate a clear innovation, deliver a consumer benefit, have a need for sandbox testing, and be ready for testing.[202] Once the firm registers, it enjoys a more flexible interpretation of FCA rules; for example, the FCA can issue regulatory guidance on a case-by-case basis or even waive entire provisions depending on the parameters of a given test.[203] The FCA believes that the relationship is mutually beneficial. While startups and their customers benefit from the certainty that their economic activity falls within legal boundaries, regulators obtain a wealth of information to use going forward.[204]

Other international jurisdictions have adopted conciliatory regulations for blockchain startups.[205] The Hong Kong Monetary Authority ("HKMA") has established its own sandbox to serve as a pilot for fintech advancements, such as blockchain, augmented reality, and

---

200. *See Regulatory Sandbox*, U.K. FIN. CONDUCT AUTHORITY (Nov. 5, 2015), https://www.fca.org.uk/firms/project-innovate-innovation-hub/regulatory-sandbox [https://perma.cc/H7F8-DDHC].

201. *See* Bloomberg View, *Bring on the Blockchain Future*, BLOOMBERG PROF. SERVS. (June 13, 2016), https://www.bloomberg.com/professional/blog/bring-blockchain-future/ [https://perma.cc/5J3M-QKQD].

202. *See Regulatory Sandbox*, *supra* note 200.

203. *See id*.

204. *See* Christopher Woolard, Dir. of Strategy & Competition, FCA, Speech at the Innovate Finance Global Summit (Apr. 11, 2016), https://www.fca.org.uk/news/speeches/innovate-finance-global-summit [https://perma.cc/97GZ-F6RD].

205. For a list of blockchain sandboxes, see Carlo R.W. De Meijer, *Blockchain: Playing in the Regulatory Sandbox*, FINEXTRA (Sept. 7, 2016), https://www.finextra.com/blogposting/13055/blockchain-playing-in-the-regulatory-sandbox [https://perma.cc/Y5B3-E7CA].

even robotics.[206] The HKMA aims to provide regulatory flexibility while still requiring participant firms to consider consumer protection and risk mitigation.[207] The Australian Securities and Investment Commission ("ASIC") created an "Innovation Hub," which it touts as a collaborative effort between financial professionals, regulators, and academics. Like the FCA, ASIC cites the costs startups face when testing a concept in a large market.[208] Fintech companies would normally need to register with ASIC to do business but would incur additional costs by modifying their business and registration status based on customer response.[209] ASIC suggests that its flexible regulatory regime can mitigate the speed-to-market problem.[210] Elsewhere in Asia, the Monetary Authority of Singapore ("MAS") has actively courted small and large blockchain enterprises as part of the country's broader Smart Nation initiative.[211] For example, MAS collaborated with the multi-firm blockchain consortium R3 to establish a "Center of Excellence" for blockchain research.[212]

The unifying theme among global regulators is cooperation between government and industry stakeholders. Unlike some of their international counterparts, regulators in the United States have rejected proposals to create their own regulatory sandboxes.[213] But there are signs of public-

206. *See* Letter from Arthur Yuen, Deputy Chief Exec., H. K. Monetary Auth., to Chief Execs., All Authorized Insts. (Sept. 6, 2016), http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160906e1.pdf [https://perma.cc/B3S5-7LC6].

207. *See id*.

208. AUSTL. SEC. & INVS. COMM'N., FURTHER MEASURES TO FACILITATE INNOVATION IN FINANCIAL SERVICES 10 (2016), http://download.asic.gov.au/media/3889025/cp260-published-08-june-2016.pdf [https://perma.cc/4AA9-UZJR].

209. *See id.*

210. *See id.*

211. *See* Diana Ngo, *Singapore Makes Blockchain a Priority*, NASDAQ (Dec. 21, 2016), http://www.nasdaq.com/article/singapore-makes-blockchain-a-priority-cm724472 [https://perma.cc/URH9-2VVZ].

212. *See* Ian Allison, *R3 Partners with Monetary Authority of Singapore, Launches Asia Blockchain Centre of Excellence*, INT'L BUS. TIMES (Nov. 9, 2016), http://www.ibtimes.co.uk/r3-partners-monetary-authority-singapore-launches-asia-blockchain-centre-excellence-1590490 [https://perma.cc/24C9-P5KE].

213. *See* Gregory Roberts, *Blockchain Not Ready for Regulatory Sandbox, Fed's Brainard Says*, Bloomberg BNA (Oct. 11, 2016), https://www.bna.com/blockchain-not-ready-n57982078299/ [https://perma.cc/V3R4-3MZW]. Federal Reserve Governor Lael

private cooperation, even if they do stop short of establishing testing environments. In addition, the Blockchain Alliance serves as a public-private forum for the Digital Chamber of Commerce to work with fintech companies to combat financial crimes that take place on blockchains.[214]

B. DERIVATIVES REGULATION UNDER DODD-FRANK AND THE COMMODITIES EXCHANGE ACT

Derivatives contracts operate both as hedging devices and pure wagers.[215] Derivatives laws often struggle to find balance between these two uses. Regulators often seek to curb over-speculation while accepting the social benefits of derivatives.[216] Prior to Dodd-Frank, the Commodity Futures Trading Commission ("CFTC") adopted a hands-off regulatory approach to derivatives under the Commodity Futures Modernization Act ("CFMA") by excluding most OTC derivatives from regulation.[217] Dodd-Frank repudiated the CFMA and instead imposed a series of requirements designed to increase both market and transaction level transparency.[218]

Under Dodd-Frank, derivatives are subject to a fragmented regulatory regime. The Securities and Exchange Commission ("SEC") asserts jurisdiction over "security-based swaps,"[219] which Dodd-Frank defines as swaps that are based on the underlying value of a security or

---

Brainard cited concerns about the maturity of the technology in rejecting a proposal for a sandbox. *Id.*

214. *See* BLOCKCHAIN ALLIANCE, blockchainalliance.org [https://perma.cc/AAN5-P93F]. This organization connects law enforcement agencies with blockchain companies. One issue facing the organization is the use of ransomware. By using ransomware, an attacker locks down a computer system and prevents a user from accessing files unless the victim pays money. Attackers often demand payment in Bitcoin, Litecoin, or other cryptocurrency since the blockchains help them preserve anonymity. *See* Danny Palmer, *How Bitcoin Helped Fuel an Explosion in Ransomware Attacks*, ZDNET (Aug. 22, 2016), http://www.zdnet.com/article/how-bitcoin-helped-fuel-an-explosion-in-ransomware-attacks/ [https://perma.cc/RWG8-VPNQ].

215. *See* Lynn A. Stout, *Derivatives and the Legal Origin of the 2008 Credit Crisis*, 1 HARV. BUS. L. REV. 1, 6 (2011).

216. *See id*. at 11.

217. *See id.* at 21.

218. *See* M. Holland West & Matthew K. Kerfoot, *The Impact of Dodd-Frank on Derivatives*, 18 FORDHAM J. CORP. & FIN. L. 269, 272 (2013).

219. *See* 15 U.S.C. § 8302(a)(2) (2012).

index of securities.[220] The CFTC has regulatory authority over all other types of swaps, including agricultural swaps.[221] The two agencies share authority over "mixed swaps," which include components of security-based swaps and other swaps.[222] Dodd-Frank does not provide a single definition for the term "swap" but lists instruments that are considered swaps and delineates several considerations in determining whether a transaction is a swap.[223] While the CFTC is the primary regulator, Dodd-Frank also affords rulemaking authority to several "prudential regulators."[224] The prudential regulators include the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Farm Credit Administration, and the Federal Housing Finance Agency.[225]

Title VII's clearing requirements represent perhaps the most consequential change to derivatives regulation. The Commodity Exchange Act ("CEA"), as amended by Dodd-Frank, now prohibits entering into a swap agreement unless that swap is submitted to a derivatives clearing organization ("DCO") or to an exempt clearinghouse for clearing.[226] Most DCOs must register with the CFTC. To do so, a registrant must comply with the CEA's seventeen core principles.[227] Once

---

220. 7 U.S.C. § 1a(42) (2012); 15 U.S.C. § 78c(a)(68) (2012).
221. *See* 15 U.S.C. § 8302(a)(1) (2012).
222. *See id.* § 8302(a)(8).
223. *See* 7 U.S.C. §§ 1a(47), 1b(a) (2012).
224. *See* 7 U.S.C. § 1a(39) (2012).
225. *See id*.
226. *See id.* § 2(h)(1)(A).
227. *See id.* § 7a-1 (2012). The seventeen core principles compel a registrant to maintain:

> 1. Adequate financial, operational, and managerial resources.
>
> 2. Appropriate standards for participant and product eligibility.
>
> 3. Adequate and appropriate risk management capabilities.
>
> 4. The ability to complete settlements on a timely basis under varying circumstances.

registered, DCOs are subject to CFTC rules regarding the implementation of these principles. For example, the CFTC mandates that DCOs maintain sufficiently liquid resources to continue to meet their financial obligations notwithstanding the default of their largest clearing member.[228] Agency rulemaking also requires DCOs to adopt procedures to contain losses in case of a clearing member's default.[229]

---

5. Standards and procedures to protect member and participant funds.

6. Efficient and fair default rules and procedures.

7. Adequate rule enforcement and dispute resolution procedures.

8. Adequate and appropriate systems safeguards, emergency procedures, and plan for disaster recovery.

9. Obligation to provide necessary reports to allow the CFTC to oversee clearinghouse activities.

10. Maintenance of all business records for five years in a form acceptable to the CFTC.

11. Publication of clearinghouse rules and operating procedures.

12. Participation in appropriate domestic and international information-sharing agreements.

13. Avoidance of actions that are unreasonable restraints of trade or that impose anti-competitive burdens.

14. Governance arrangements and fitness standards.

15. Rules to minimize conflicts of interest in the DCO's decision-making process, and a process for resolving any conflicts.

16. Composition of governing boards to include market participants.

17. Well-founded legal framework for the activities of the DCO.

Clearing Organizations, U.S. COMMODITY FUTURES TRADING COMM'N, http://www.cftc.gov/industryoversight/clearingorganizations/index.htm [https://perma.cc/AJX9-Q7CS].

228. *See* 17 C.F.R. § 39.11(a)(1), (e) (2016).

229. *See id.* § 39.16.

The CEA charges the CFTC with reviewing swaps and determining whether they should be subject to mandatory clearing (these are called "designated swaps").[230] The CFTC can independently review classes of swaps and determine whether they should be subject to clearing; it can also initiate review when a DCO submits reports of swaps it plans to clear. The CEA lists a number of factors for the CFTC to consider in determining whether to designate a swap for clearing.[231] The major statutory exception to the CEA's clearing requirements is known as the commercial end-user exception. It applies to swaps where one counterparty "(i) is not a financial entity; (ii) is using swaps to hedge or mitigate commercial risk; and (iii) notifies the Commission . . . how it generally meets its financial obligations associated with entering into non-cleared swaps."[232] The exception is designed for non-financial users who use the swap for hedging purposes and can sufficiently prove their ability to meet their obligations. Invoking this exception is optional, and the decision to do so rests entirely on the counterparty meeting all three criteria.[233]

Even if a class of swaps is required for clearing and not subject to an exception or exemption, some highly customized OTC derivatives lack sufficient liquidity to be accepted for clearing. For these swaps, Dodd-Frank requires the Prudential Regulators to propose unified margin requirements for uncleared swaps within their scope of authority.[234] In addition, the CFTC and the SEC are charged with issuing their own margin requirements for uncleared swaps that are not subject to Prudential Regulator oversight.[235]

Once trades are cleared, or granted an exemption, they are subject to Dodd-Frank's post-trade reporting and document retention requirements. The amended CEA requires all swaps, whether cleared or uncleared, to be reported to a swap data repository ("SDR").[236] According to CFTC regulation, swap participants are also subject to ongoing reporting

230. *See* 7 U.S.C. § 2(a)(1) (2012).
231. *See id.* § 2(h)(2)(D).
232. *Id.* § 2(h)(7)(A).
233. *See id.* § 2(h)(7)(B).
234. *See id.* § 6s(e)(2)(A).
235. *See id.* § 6s(e)(2)(B).
236. *See id.* § 2(a)(13)(G).

obligations. At the outset, reporting parties must send electronic swap creation data to SDRs.[237] Swap creation data includes data regarding the agreement's terms. [238] In addition, reporting parties must send continuation data to SDRs.[239] This includes data concerning any changes to the swap's economic terms, including data pertaining to life cycle events and valuation.[240]

III. BLOCKCHAIN'S IMPACT ON SYSTEMIC RISK

Depending on the technology's development, blockchains could radically revamp the market structure for derivatives trades. Existing regulations may not be sufficient to address the risks posed by a blockchain derivatives market. It is difficult, and arguably counterproductive, at this stage of the blockchain's development to suggest concrete proposals for new rules. Instead, this part argues that systemic risk is the primary concern driving current derivatives regulation and that a new regulatory scheme must consider blockchain's unique risks. This part argues that CCPs, while generally seen as an effective way to reduce systemic risk, partially create risk by creating large central entities that are subject to failure. While blockchains can reduce the risk of over-centralization, this part warns that blockchain technology may create systemic risks of a different nature. Regulators must consider these risks when determining how to govern blockchain markets.

A. CENTRALIZATION AND SYSTEMIC RISK

One of regulators' chief concerns regarding derivatives is their role in enhancing financial systemic risk.[241] There is no single definition for systemic risk. Oftentimes, it is defined according to its consequences: bank runs, payment crises, failures of interconnected firms, and general

237. *See* 17 C.F.R. § 45.3 (2016).
238. *See id.* § 45.1.
239. *See id.* § 45.4.
240. *See id.* §§ 45.1, 45.4.
241. *See Regulatory Reform and the Derivatives Market*, *Hearing Before the S. Comm. on Agriculture, Nutrition and Forestry*, 111th Cong. 3 (2009) (statement of Tom Harkin, Chairman of S. Comm. on Agriculture, Nutrition, and Forestry).

distrust in the financial system.[242] Alternatively, systemic risk may be expressed in terms of potential causes, such as a company being "too big to fail, too interconnected to fail, or too leveraged to fail."[243]

Systemic risk is traditionally associated with institutional failure. Banks and other financial intermediaries provide market access, so widespread institutional failure can increase costs of capital.[244] Bank runs can signal institutional systemic risk.[245] A panic among depositors can trigger requests for withdrawals, and because banking assets are primarily long term, banks do not hold enough cash to satisfy demands.[246] This can force some banks into bankruptcy, but since banks often lend to one another, a defaulting bank can renege on its obligations to another institution.[247] In a panic, multiple defaults can reverberate across the entire industry, ultimately causing a "domino effect" of failures.[248]

Despite its strengths, the central clearing model is viewed skeptically by many commentators. Dodd-Frank skeptics suggest that it is unclear whether the concentration of risk in central entities is ultimately good or bad for systemic risk. The blockchain's potential to distribute tasks traditionally conducted by CCPs reopens the discussion about risks posed by centralization.[249] This worldwide mandate saddles CCPs with hundreds of trillions of dollars' worth of additional trades that would not have required clearing prior to the financial crisis.[250]

---

242. *See* SCALCIONE, *supra* note 130, at 85-87.

243. *See Perspectives on Systemic Risk*, *Hearing Before the H. Subcomm. on Capital Markets, Insurance, and Government Sponsored Enterprises of the Comm. of Financial Services*, 111th Cong. 2 (2009) (statement by Paul Kanjorski, Chairman of the Subcomm. on Capital Markets, Insurance, and Government Sponsored Enterprises).

244. *See* Steven L. Schwarcz, *Systemic Risk*, 97 Geo. L.J. 193, 199 (2008).

245. *See* SCALCIONE, *supra* note 130, at 85.

246. *Id.*

247. *Id.*

248. *Id.*

249. *See* Mark J. Roe, *Clearinghouse Overconfidence*, 6 CAL. L. REV. 1641, 1675 (2013).

250. *See* Hester Plumridge, *What if a Clearinghouse Failed?*, WALL ST. J. (Dec. 2, 2011), http://www.wsj.com/articles/SB10001424052970204397704577074023939710652 [https://perma.cc/59ZT-PG85].

By their very function, CCPs are inherently interconnected to numerous financial institutions.[251] In a way, "clearing has turned out to be the Mother of All Interconnections, because every big financial institution is connected to all big CCPs, and . . . everyone has to funnel the bulk of their derivatives trades through clearinghouses." [252] The CCP's membership will almost invariably consist of large firms that, in turn, have their own large customers.[253] While margin calls and loss sharing rules can alleviate some of the stress of a member firm's failure, CCPs are still vulnerable to failures by particularly large member firms that serve multiple functions.[254] In addition to serving as general members, some members serve as depository banks, custodians, and settlement banks.[255] During a crisis, these firms must manage their own operations in addition to supporting the CCP with variation margins.[256]

The problem is compounded by CCPs' mandated acceptance of swaps that are comparatively less liquid. The relative illiquidity of certain types of swaps can sometimes make variation margin calculation an imperfect science, as the CCPs would need to introduce models into their pricing formulae.[257] In a worst-case scenario, multi-function clearing members could default and fail to meet variation margin requirements on time.[258] As a result, the clearing mandate could leave CCPs vulnerable to liquidity shortages during periods of financial stress.[259] Such a shortage would compromise the CCPs' ability to meet their obligations towards

---

251. *See* Hester Peirce, *Derivatives Clearinghouses: Clearing the Way to Failure*, 64 CLEV. ST. L. REV. 589, 621 (2013).

252. Craig Pirrong, *The Fifth Year of Frankendodd*, STREETWISE PROFESSOR (July 21, 2015), http://streetwiseprofessor.com/?p=9472 [https://perma.cc/FF6B-WX7C].

253. *See* Peirce, *supra* note 251, at 621.

254. *See* Froukelien Wendt, *Central Counterparties: Addressing Their Too Important to Fail Nature* 9 (Int'l Monetary Fund, Working Paper No. WP/15/21, 2015), https://www.imf.org/external/pubs/ft/wp/2015/wp1521.pdf [https://perma.cc/B5K3-H64T].

255. *See id*.

256. *See id*.

257. *See* Griffith, *supra* note 122, at 1316.

258. *See* Patrick Parkinson, Remarks Delivered to Federal Reserve Bank of Chicago Annual Over the Counter Derivatives Symposium: CCP Liquidity Risk Management and Related Failure Management Issues 2-3 (2014), https://www.chicagofed.org/~/media/others/events/2014/annual-over-the-counter-derivatives-symposium/parkinson-ccp-derivatives-over-the-counter-2014-pdf.pdf [https://perma.cc/G55U-MJF8].

259. *See* Pirrong, *supra* note 252.

non-defaulting members. These events do not occur in a vacuum; a CCP's failure to meet its obligations could undermine confidence in the markets in which it provides clearing services.[260] Thus, its failure could very well result in the type of financial contagion that it was designed to protect against in the first place.

The blockchain's decentralization of clearing functions could reduce the risks posed by excessive centralization. One of the guiding tenets of the blockchain is its lack of a single point of failure. The ideal blockchain-based system can decentralize key clearing functions and distribute those tasks among members of the network. Blockchain entrepreneurs are optimistic that smart contracts can automate integral processes including matching and affirmation, collateral management, default management, and settlement.[261] The results of this could be profound, as CCPs would play a diminished role or even be displaced altogether. Skeptics note that blockchains cannot replicate every CCP process; CCPs mutualize default risk and manage positions in a way that blockchains presently cannot.[262] While it may currently be the case that blockchains cannot emulate the diverse array of CCP functions, the potential benefits of disintermediation could be too tantalizing to ignore. Blockchains can be incorporated into existing processes for efficiency gains, and industry partnerships and new startups are constantly pushing the technology towards greater levels of disintermediation.

B. THE SYSTEMIC RISKS POSED BY DECENTRALIZED SYSTEMS

Blockchain evangelists continue to make advancements to the technology through industry-wide cooperation on research. As practical application of the technology comes closer to fruition, the CFTC and its international counterparts must consider whether the current regulatory paradigms can apply to this new technology. If the technology lives up to the lofty expectations posed by some of its enthusiastic entrepreneurs, then certain requirements, such as mandated central clearing, could become obsolete. Certain markets, such as those for uncleared OTC swaps, would be far more transparent than they are today.[263] While

260. *See* Parkinson, *supra* note 258, at 3.

261. *See* Parsons, *supra* note 181.

262. *See* Craig Pirrong, *A Pitch Perfect Illustration of Blockchain Hype*, COINDESK (Oct. 16, 2016), http://www.coindesk.com/a-pitch-perfect-illustration-of-blockchain-hype/ [https://perma.cc/AH6L-YZ46].

263. *See* COMMODITIES FUTURES TRADING COMM'N, *supra* note 174, at 195.

regulators and market participants may salivate over blockchain's potential, they must also realize this change in market structure is not a riskless proposition. Although the risks of over-centralization are well-documented in legal scholarship and blockchain's disintermediation of settlement procedures seems to directly address those concerns, this decentralized structure comes with risks of its own.

Though it may be too early to pose a new regulatory regime, there are some themes to evaluate when considering ways to regulate blockchain markets. Systemic risk will still exist in blockchain markets; only the sources of systemic risk will change. Decentralization of market intermediaries shifts regulatory concern from the systemic risks created by interconnected institutions to those inherent in the market itself. In addition, such a heavy reliance on digital trading infrastructure suggests that the market structure could be a source of risk.

The CFTC should focus on its regulatory prerogative to reduce systemic risk, which has taken precedence since the enactment of Dodd-Frank.[264] Regulators must account for the unique risks posed by a decentralized network. They can do so by addressing issues regarding settlement finality and recourse, especially in the context of potential cyberattacks on the blockchain network. In addition, regulators should be cognizant of the type of behavior that could arise as market participants take advantage of the blockchain's efficiencies. The CFTC should remain vigilant in requiring reporting by swap participants. Blockchains can enhance this functionality if regulations are updated to allow reporting through the shared ledger.[265]

Blockchain transactions lack certain crucial elements of traditional legal agreements. They are transparent and easily verifiable. For example, to allow communal payment verification to take place, Bitcoin attempts to ensure that transactions are irrevocable—no *single* user could reverse a transaction after it is entered into the blockchain ledger. But the unidirectional nature of these transactions becomes a liability in the event of a disputed transaction. Bitcoin manages to prevent illegitimate

---

264. *See generally Perspectives on Systemic Risk: Hearing Before the H. Comm. on Financial Services*, 111th Cong. (2009).

265. *See* Jenny Cieplak & Mike Gill, *How Distributed Ledgers Impact Post-Trade in a Dodd-Frank World*, COINDESK (July 9, 2016), http://www.coindesk.com/distributed-ledger-cftc-post-trade-dodd-frank/ [https://perma.cc/7TG7-VBXV].

payments, but this is of little use if the transfer is based on fraudulent pretenses to begin with.[266] Even after the transaction is finalized, if a court orders damages arising from, for example, a fraudulent transfer, the initial transaction is not "undone," per se. Instead, the party that must pay the damage award would initiate a new transaction in the amount owed, or face further judicial sanctions.[267] The Bitcoin blockchain itself cannot resolve this problem internally; it must rely on other remedies, such as those imposed judicially, to deal with fraudulent transfers.

Immutability, despite being an important part of Bitcoin functionality, is a malleable concept. Once a transaction is finalized and placed into the public ledger, a subsequent, prohibited transaction, such as a double spend, would fail scrutiny under the proof of work process. But since blockchains are, in effect, communal verification mechanisms, it is possible for cabals of bad actors to impose their version of the truth onto the network. This problem can manifest itself through the blockchain's main technological vulnerability, called the "51% attack."[268] The basic premise of this exploit is that if a single attacker or group of attackers controlled more than 50% of the blockchain's computing power, they could produce hashes at a fast-enough rate to overwrite other users' transactions.[269] Thus, a malicious user that controls 51% of the blockchain's mining hash-rate could theoretically send a transaction and then reverse it.[270] The blockchain would suggest that this malicious user still possessed an asset when, in fact, that asset had just been transferred.

---

266. *See* SWAN, *supra* note 16.

267. *See* John Servidio, *Blockchain: Why It Matters for Financial Services Lawyers*, LAW360 (Aug. 18, 2016), https://www.law360.com/articles/830173/blockchain-why-it-matters-for-financial-services-lawyers [https://perma.cc/XYT3-KHMS]. Court orders and subpoenas can present other problems with privacy and data security. Though blockchains are theoretically anonymous, a court order or subpoena could expose a party's private key, thus exposing personal information. *See* Donald B. Johnston, *More on the Law and Blockchain*, LEXOLOGY (Apr. 11, 2016), http://www.lexology.com/library/detail.aspx?g=ee10aa0f-3447-4088-81dd-7521244fecb3 [https://perma.cc/7BDG-DJ9L].

268. *See Weaknesses*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Weaknesses [https://perma.cc/QW7Y-BXJM] (describing the capabilities of a Bitcoin attacker with more than 50% of a network's computing power).

269. *See id*.

270. *See id*.

Undoing blockchain errors is not a simple task. As of this writing, the highest profile attack and attempted resolution of a blockchain attack involved Ethereum. The attack on Ethereum was not a 51% attack but rather an exploit in the programming language that facilitates smart contract creation.[271] This attack is perhaps the greatest security challenge to a cryptocurrency to date. Some observers attribute the attack to the flexibility Ethereum affords its users.[272] While Bitcoin's programming language is sufficient to effectuate relatively simple currency transactions, Ethereum allows users to use several languages to create more sophisticated agreements.[273] Some suggest that this led to vulnerabilities in the underlying smart contract code.[274] The attacker managed to drain millions of Ether from Ethereum's largest distributed autonomous organization—a crowdfunding pool named, "The DAO."[275] Users who invested in The DAO's projects quite literally watched, on the blockchain, as the attacker siphoned off funds to another address.[276] In an open letter to Ethereum's users, the hacker took refuge in the immutability of the smart contract by suggesting that he or she cannot be subject to any additional legal obligations beyond those codified in the coded agreements at issue.[277]

The legal merit of such a claim is far from clear, but Ethereum nonetheless took action by creating a "fork."[278] Ethereum blacklisted the offending addresses and offered a firmware update to its remaining user base.[279] This solution effectively created two blockchains: one with the most recent update and another that was theoretically obsolete.[280] Of

---

271. *See* David Siegal, *Understanding the DAO Attack*, COINDESK (June 25, 2016), http://www.coindesk.com/understanding-dao-hack-journalists/ [https://perma.cc/BB7R-BZHA].

272. *See id*.

273. *See id*.

274. *See* Joseph Young, *Ethereum Smart Contract Issues Frustrate Developers with Fatal Bugs*, CRYPTOCOINS NEWS (Nov. 12, 2016), https://www.cryptocoinsnews.com/ethereum-smart-contract-issues-frustrate-developers-fatal-bugs/ [https://perma.cc/BSH4-L5NH].

275. *See id*.

276. *See id*.

277. *See id*.

278. *See* Siegal, *supra* note 271.

279. *Id.*

280. *See id.*

course, the viability of a blockchain fork depends on the users installing the update; Ethereum cannot compel users to do so. An attacker can exploit this vulnerability by promising users incentives to remain on the old version of the blockchain.[281] The long-term effects of this solution are unclear. On the one hand, the hard fork splits the community, and an intervention of this magnitude could undermine faith in the currency going forward. Then again, a hard fork is perhaps the more palatable solution compared to the alternative of losing millions. Critics question how the fork will affect the perception of Ethereum and blockchains as secure payment mechanisms going forward, with some going so far as to call it a bailout.[282]

The concerns about cyber-attacks and the Ethereum fork bring to light one of the main disputes regarding blockchains: the notion of settlement finality. Broadly speaking, settlement finality is the moment at which a transaction becomes final and irreversible.[283] Finality is important to financial firms because it provides certainty as to when assets are legally theirs.[284] Parties thus rely on the concreteness of finality to determine asset ownership and monitor risks.[285]

Blockchains challenge traditional notions of finality. As Ethereum founder Vitalik Buterin writes, "decentralized systems . . . may [definitively provide settlement finality], or they may provide it probabilistically, within certain economic bounds, or not at all."[286] Depending on the design of the blockchain, finality can be amorphous. In a consensus-based proof of work system, it is difficult to predict the future

---

281. *See id*.

282. *See id.*; Frances Coppola, *A Painful Lesson for the Ethereum Community*, FORBES (July 21, 2016), http://www.forbes.com/sites/francescoppola/2016/07/21/a-painful-lesson-for-the-ethereum-community/#58f1bc435714 [https://perma.cc/WQH7-33NH].

283. *See* DAVID MILLS ET AL., DISTRIBUTED LEDGER TECHNOLOGY IN PAYMENTS, CLEARING, AND SETTLEMENT 31 (2016), https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf [https://perma.cc/5YL2-Q9UN].

284. *See* Vitalik Buterin, *On Settlement Finality*, ETHEREUM (May 9, 2016), https://blog.ethereum.org/2016/05/09/on-settlement-finality/ [https://perma.cc/U25Q-RATW].

285. *See* MILLS ET AL., *supra* note 283, at 32.

286. *See* Buterin, *supra* note 284.

security of a transaction that has been incorporated into a block.[287] There is always the possibility that an actor or several actors working in concert could assume most of the blockchain's mining power, giving them the ability to rewrite blocks and undo previously settled transactions.[288] While the term "51% attack" likely evokes images of an attack by a flood of hackers, such an attack need not originate from external actors. Consider Bitcoin's blockchain, where the difficulty of the proof of work problem largely depends on the network assigning a target value.[289] The blockchain sets the target value, and this determines the difficulty of the proof of work problem. Recall that Bitcoin assigns the target according to the number of miners on the network; the proof of work problem thus becomes more difficult as more people connect to the network and become stakeholders.[290] This creates a situation where the "level of security . . . is directly proportional to the future value of the token, which is unknowable."[291] As the difficulty of the proof of work problem changes, transactions may become easier (or more difficult) to reverse.

Many blockchain stakeholders suggest that using private or consortium blockchains sufficiently mitigates this problem. Bitcoin and Ethereum use public blockchains, allowing any person with a computer to download the client, participate in the mining process, and read the ledger.[292] The consensus process and the determination of the blockchain's truth is left up to the public via cryptography and economic incentives.[293] Conversely, private blockchains tightly control access via a central administrator.[294] The administrator can distribute read permissions

---

287. *See* Tim Swanson, *Settlement Risks Involving Public Blockchains*, TABB FORUM (Mar. 24, 2016), http://tabbforum.com/opinions/settlement-risks-involving-public-blockchains [https://perma.cc/WFH6-PYJH].

288. *See id*.

289. *See* NAKAMOTO, *supra* note 1, at 3.

290. *See id*.

291. *See* Swanson, *supra* note 287.

292. *See* Vitalik Buterin, *On Public and Private Blockchains*, ETHEREUM (Aug. 7, 2015), https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ [https://perma.cc/T2AY-38L9].

293. *See id.*

294. *See* Luke Parker, *Public Versus Private Blockchains: Is There Room for Both to Prevail?*, MAGNR BLOG (Apr. 21, 2016), https://magnr.com/blog/technology/private-vs-public-blockchains-bitcoin/ [https://perma.cc/328A-4NZB].

(the ability to view the blockchain) to pre-approved parties.[295] Ultimately, however, only the administrator can write (or input) new transactions to the blockchain.[296] Consortium blockchains serve as something of a middle ground between the two extremes: they allow consensus by permitting only a certain number of trusted nodes to engage in the verification process.[297] Because a consortium blockchain requires some element of pre-screening and familiarity among participants in the consensus process, members can hold one another accountable for modifications to the ledger. Consortium blockchains cannot completely resolve finality issues, however. For example, a blockchain cannot prevent collusion among members of a settlement consortium.[298] There are historical examples of collusion among financial firms, including the notable and relatively recent case of LIBOR rate manipulation among London banks.[299]

The lack of transaction finality can be a major source of systemic risk in a decentralized system. As disintermediation occurs, systemic risk "should increasingly be viewed by its impact on markets, not institutions."[300] Risks of this nature increase costs of capital for market participants, even if an initial shock occurs at an institution that is not a major source of market access.[301] Ideally, financial institutions insulate themselves from risk through diversification; they invest in assets that have a negative correlation, or no correlation, to each other and the market.[302] The net result should be a portfolio that has little to no net risk. A market-based systemic risk can be positively correlated with the market. For example, Steven Schwarcz considers the near-failure of the

---

295. *See id.*

296. *See id.*

297. *See* Buterin, *supra* note 292.

298. *See* Phil Gomes, *A Morning Exploration of Blockchain Technology in Financial Services*, EDELMAN (Nov. 23, 2016), http://www.edelman.com/post/exploration-blockchain-technology-financial-services/ [https://perma.cc/XK35-ACNL].

299. *See* Liam Vaughan & Gavin Finch, *Libor Scandal: The Bankers Who Fixed the World's Most Important Number*, GUARDIAN (Jan. 18, 2017), https://www.theguardian.com/business/2017/jan/18/libor-scandal-the-bankers-who-fixed-the-worlds-most-important-number [https://perma.cc/U394-F422].

300. Schwarcz, *supra* note 244, at 202.

301. *See id*. at 201.

302. *See id*. at 200.

infamous hedge fund Long-Term Capital Management ("LTCM") as an illustration of this type of risk. While LCTM perhaps suffered from some "hubris" by taking on increasing amounts of leverage, its diversified positions ultimately failed "as the entire market moved in the same direction at the same time."[303] Thus, instead of its losses being offset, they were magnified and transmitted to its counterparties through its derivatives positions.[304]

A lack of finality is a type of systemic risk that affects the market. Without a clearly defined moment of finality, it may be difficult to determine liability if a participant in a blockchain agreement suffers insolvency.[305] The Bank for International Settlements' Core Principles for Systemically Important Payment Systems call for definitive finality because participants can face liquidity risk if they are unable to transfer the settlement asset for another claim.[306] This can have systemic effects because "all participants holding the settlement asset are [simultaneously exposed to liquidity risk] and . . . market participants can have little control over the timing and size of their holding of the settlement asset."[307] In adopting its own settlement finality directive, the then European Commission recognized that without definitive finality, the insolvency of a single participant could cause liquidity concerns across an entire payment, which would in turn undermine confidence in the entire market.[308] Ensuring definitive finality can be a way to foster confidence in markets[309] and prevent the positively correlated market movements that would occur from a loss in confidence (which would render hedging positions ineffective).

Regulators can provide clarity around finality. While it is perhaps too early in the blockchain's technological life to create a new and specifically tailored regime for settlement finality, it is possible to

303. William McDonough, President, Fed. Reserve Bank of N.Y., Statement Before the Comm. on Banking & Fin. Servs. (Oct. 1, 1998).

304. *See* Schwarcz, *supra* note 244, at 201.

305. *See* MILLS ET AL., *supra* note 283, at 31.

306. *See* BANK FOR INT'L SETTLEMENTS, CORE PRINCIPLES FOR SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS 31 (2001), http://www.bis.org/cpmi/publ/d43.pdf [https://perma.cc/T8RF-KSLZ].

307. *Id*. at 34.

308. *See* Swanson, *supra* note 287.

309. *See id*.

envision ways in which the current regulatory regime can adapt to changes in market infrastructure. Regulators cannot rest on their laurels and expect the blockchain to resolve every problem. To the contrary, in some ways, it appears that decentralizing clearing and settlement processes substitutes one type of systemic risk for another. Under a centralized clearing structure, the primary source of systemic risk stems from a crucial intermediary's exposure to other institutions. In a decentralized and distributed blockchain system, systemic risks will likely come from losses in market confidence caused by disputes in finality.

The idea that regulators could serve as limited permission nodes on the blockchain is commonly floated among the blockchain community.[310] This potentially gives regulators access to a wealth of data that they would otherwise not have, even under the current reporting regime. The ledger itself can serve as the record for swap transactions, and can store both creation and ongoing data required by the CFTC's reporting rules.[311] This arrangement can result in major efficiencies. Currently, there are four CFTC-registered SDRs, each of which uses different software and reporting architecture, making it difficult for the CFTC to aggregate and analyze data. [312] A blockchain consisting of prominent market participants could comply with the requirements and provide transparency in the form of viewable, standardized data.[313]

The nature of blockchains and the potential risk factors associated with their use suggest that regulators may need to be even more proactive in adapting the current regulatory scheme to the emerging technology. Mitigating systemic risk in blockchain systems will likely require regulators to set new standards for the underlying smart contracts. This may require the CFTC and other agencies to take a hands on approach to cyber security issues and problems relating to the blockchain's technological infrastructure.

---

310. *See* Nikiforos Matthews & Jonas Robison, *Recent Blockchain Regulatory Developments*, ORRICK, HERRINGTON & SUTCLIFFE: DERIVATIVES REV. (Jan. 31, 2017), http://blogs.orrick.com/derivatives/2017/01/31/recent-blockchain-regulatory-developments/ [https://perma.cc/P45Z-ZXSR].

311. *See* 17 C.F.R. § 45.3 (2016).

312. *See* Cieplak & Gill, *supra* note 265.

313. *See id*.

Smart contracts and blockchains are financial innovations that regulators must stay ahead of. If derivatives markets move to blockchain architecture, counterparties could adopt new types of agreements. While financial innovation is typically thought of in terms of the development of new products, advances in market structure can achieve the same result. Financial innovation can occur when there are changes in markets and intermediaries that affect the way that counterparties manage risk.[314] This is founded in Ronald Coase's economic theory, which suggests that firms and markets are substitutes for economic production and that, without transaction costs, economic production would occur entirely through markets.[315] New products create ways for actors to move their risks to markets; while bespoke at first, the market's demand for these instruments leads to standardized, liquid forms of these arrangements.[316]

Thus, a fundamental change to the market's technological infrastructure could also be characterized as financial innovation in this sense. The blockchain promises to simplify the creation of new instruments. Swap creators can easily emulate the term structures of other securities and use the blockchain's computational power to automatically make appropriate margin adjustments. Blockchain's proponents suggest that this will lead to the creation of new types of agreements, allowing firms to transfer new types of risk.[317] While this provides a way for firms to move more risks off their balance sheets, the usual result of financial innovation is information asymmetry between market participants and regulators.[318] Typically, the source of the asymmetry is the regulators' inability to ascertain the risks posed by these new instruments; standardization can be a way to reduce these asymmetries. [319] Blockchains, however, provide something of a twist to this formula. Regulators can mitigate some of the risks posed by the terms of the new instruments by serving as nodes, but the contract's code can serve as a new source of risk.

Until smart contracts become industry staples, the CFTC should closely scrutinize them. ISDA currently plays a prominent role in contract standardization, but smart contracts may necessitate an additional level of review in their early lives. The Ethereum situation is an interesting case

---

314. *See* Gubler, *supra* note 124, at 61.
315. *See id*. at 69.
316. *See id*. at 69-70.
317. *See* WYMAN, *supra* note 167, at 10.
318. *See* Gubler, *supra* note 124, at 106.
319. *See id*.

study in the potential pitfalls of smart contract vulnerability. Since the hack occurred relatively recently, the long-term effects on user confidence in the Ethereum network are unclear. But given the potentially systemic repercussions that the lack of finality can have on the market, regulators may not want to take risks with the new technology. One way to cut off a source of risk would be to regulate the smart contracts themselves, in the same way that CFTC regulation compels reporting of swap terms to SDRs. The unique risks posed by smart contracts may additionally require the CFTC to review the underlying smart contract code to screen for vulnerabilities.

CONCLUSION

Blockchain technology is still very much evolving. Both finance firms and regulators are still exploring the specific ways in which blockchains can benefit capital markets. At this stage, it is perhaps best that regulators allow the technology to develop in its natural course. At the same time, it would benefit regulators to remain on the legal cutting edge by understanding the potential promises and pitfalls of the technology. The efficiencies provided by blockchains are substantial, as they could reduce transaction costs across the board for derivatives market participants. They can also remove or reduce reliance on central counterparties that are exposed to large amounts of credit risk. But blockchains are not without problems of their own. Technological vulnerabilities can create new systemic risks, which regulators must be prepared to mitigate *before* a financial crisis occurs. The specifics of any prophylactic measures will largely depend on how the technology develops, but what is clear right now is that an analysis of blockchains' systemic risks will likely require an understanding of data and code as much as of finance and the law.