Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues

Elizabeth Sara Ross

The Catholic University of America, Columbus School of Law
NOBODY PUTS BLOCKCHAIN IN A CORNER: THE DISRUPTIVE ROLE OF BLOCKCHAIN TECHNOLOGY IN THE FINANCIAL SERVICES INDUSTRY AND CURRENT REGULATORY ISSUES

Elizabeth Sara Ross †

“Technology changes. Economy laws do not.”

INTRODUCTION

Recall the old VISA commercials portraying a modern consumer’s synchronized and effortless credit card transactions undermined by the one Luddite with the audacity to bring the marketplace to a grinding halt by presenting cash (or worse, a check). By visualizing faster and more efficient payments, consumers would transition to credit cards for their convenience, not because it was a safer or more secure option. Rather than emphasize the credit card itself, VISA’s viscerally engaging and forward-looking advertisement allowed consumers to imagine heightened human experiences made possible because of technology. Fast-forwarding to our modern brave new world, our financial ecosystem and definition of “trust” have rapidly changed. People engage

†J.D. Candidate, May 2018, The Catholic University of America, Columbus School of Law; B.A. 2015, Rhodes College. The author would like to extend her deep gratitude to Professor Heidi M. Schooner for her mentorship, expertise, and invaluable guidance in drafting this Note. The author is also grateful to her colleagues on the Catholic University Journal of Law and Technology for their contributions to this Note. Lastly, the author wishes to thank her parents for their unwavering love, patience, and support during the writing process and throughout law school.


3 See OLIVER E. WILLIAMSON, THE MECHANISMS OF GOVERNANCE 256-57 (Oxford
socially,\textsuperscript{3} take food from,\textsuperscript{6} get into cars with,\textsuperscript{7} and inhabit the homes of strangers.\textsuperscript{8} The invention of the Internet, paired with the mass proliferation of mobile phones,\textsuperscript{9} has transformed consumer financial conduct\textsuperscript{10} and cultivated a
societal expectation of progress as determined by the level of convenience.\textsuperscript{11} Why? Companies are cognizant of the new peer-to-peer services (“P2P”) code of the sharing economy;\textsuperscript{12} get rich or adapt trying.\textsuperscript{13}

Following the global financial crises of 2007-2009,\textsuperscript{14} the world’s trust in banks was at an all-time low.\textsuperscript{15} Capitalizing on this time, Satoshi Nakamoto\textsuperscript{16} (a person or an entity) pseudonymously released Bitcoin\textsuperscript{17} to replace the traditional role of the banker\textsuperscript{18} and provide a more transparent, equitable, and efficient payment system.\textsuperscript{19} The range of Bitcoin’s initial negative publicity, including price volatility,\textsuperscript{20} hacking,\textsuperscript{21} fraudulent investment schemes,\textsuperscript{22} and black market

\begin{thebibliography}{9}
\bibitem{11} Consumers cite that “convenience” is the most common reason motivating their adoption of mobile payment activity. \textit{See Board of Governors of the Federal Reserve System, Consumers and Mobile Financial Services 2016 (Mar. 2016).}
\bibitem{13} Chris Skinner, \textit{ValueWeb 162} (2016) (“Apps and mobile are changing the retail experience; [Application Program Interfaces] are shifting the operations to real-time processing; and cloud, combined with data analytics are changing product and service.”); \textit{see also} David McBride, \textit{General Corporation Laws: History and Economics, Law & Contemp. Probs.} 1, 9-10 (2010) (analyzing the economic evolutionary effects of how physical technologies, social technologies, and business organization interact and coevolve); \textit{Eric Beinhocker, The Origin of Wealth: Evolution, Complexity and the Radical Remaking of Economics} 15 (2006) (recognizing “social technologies” as “ways of organizing people to do things”).
\bibitem{14} \textit{See Hal Scott, Connectedness and Contagion} (MIT Press 2016).
\bibitem{16} It has been theorized that “the name might be a portmanteau of four technology companies: Samsung, TOSHiba, NAKAmichi, and MOTOrola.” \textit{David Lee Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data} 11, n.1 (2015).
\bibitem{18} Brian Kelly, \textit{The Bitcoin Big Bang} 79 (2015).
for the deep web, conditioned the public’s perception of all cryptocurrencies with illicit purposes. Despite bitcoin’s “growing pains,” venture capitalists, software developers, and technology start-up companies continued to assert...


23 The currency’s association with Silk Road created the misconception that all bitcoin is linked to money launderers and terrorists.


26 “Bitcoin represents not only the future of payments but also the future of governance.” CHI SKINN ER, VALUEWEB 99 (2016) (quoting Dee Hock, Founder of Visa). See also Marc Andreessen, Why Bitcoin Matters, N.Y. TIMES (Jan. 21, 2014), https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/. The practical consequence of solving this problem is that Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.


that the true value of Bitcoin is the blockchain, the distributed ledger technology ("DLT") in which the bitcoin currency operates. Previous discussions surrounding blockchain were initially constrained to educating others on how the technology worked and hype" over the potential applications that might be implemented in the distant future. While it was previously speculated that the financial services and banking industries would have to wait five to ten years before the potential of blockchain technology was actually turned into a reality, IBM released a report stating that “2017 looks to be the year banking on blockchain’s shifts from zero to sixty.” Accordingly, the global competition to service distributed ledger technology by incorporating it into the existing financial services industry is advancing in real time. The World Economic Forum estimates that more than 25 countries are investing in blockchain technology, filing more than 2,500 patents and investing $1.3 billion. Regu-


31 See Nicole Bullock, Blockchain starts transition from hype to everyday use in markets, FIN. TIMES (Oct. 10, 2016), https://www.ft.com/content/08d54dc7-74e2-11e6-bf48-b372cdeb1043a; How Coin Center Is Helping Define The ‘Big Fuzzy Gray Area’ Of Blockchain And Cryptocurrency Law, TUNEIN (Oct. 18, 2016), http://tunein.com/embed/player/t109377177/ (discussing how one of the ways CoinCenter represents bitcoin blockchain technology, includes ensuring that policy makers “understand the technology and don’t do anything stupid” by “mak[ing] easy to avoid mistakes”).


33 J. Christopher Giancarlo, Commissioner, U.S. Commodity Futures Trading Comm’n, Address to the American Enterprise Institute, 21st Century Markets Need 21st Century Regulation (Sept. 29, 2016), http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-17 (acknowledging that in comparison to international regulatory efforts that have been effected to address distributed ledger technology, the United States is “falling behind”).


latory interest in financial technology (“FinTech”) in the United States represents a turning point, in which the focus shifts from attempting to prevent the previous crises, to looking at how to support future market developments while maintaining financial stability.

Blockchain technology has been frequently, and appropriately, analogized to the Internet Protocol. The potential of each respective protocol is realized after the application of a new layer of services on top of the technology. Similar to how the Internet fundamentally changed the way we share information, blockchain is an open source innovation that is going to revolutionize the transactions among individuals, governments, businesses, and machines.


Philip Stafford, Banks struggle to make blockchain fast and secure, WALL ST. J. (Sept. 26, 2016), http://www.ft.com/cms/s/2/e0a32840-4f68-11e6-8172-e39ec3b86fc.html#axzz4tNgVau0.


Id.

Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the S. Comm. On Homeland Sec. and Gov’t Aff., 113th Con. 5 (2013) (Statement of Patrick Murck, General Counsel, The Bitcoin Foundation). “Bitcoin is a protocol. It is like TCP/IP, which enables all the different uses people around the globe invented for the Internet. And it is like HTML, which enables all the different uses people invented for the World Wide Web without having to ask anyone’s permission. We envision Bitcoin as a driver of global change that rivals these other protocols in terms of the benefits it delivers to humankind across the globe.” Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the S. Comm. On Homeland Sec. and Gov’t Aff., 113th Con. 5 (2013) (Statement of Patrick Murck, General Counsel, The Bitcoin Foundation).

See Kelly, supra note 18, at 77. Services include social engagement, (Facebook), entertainment (iTunes), information (Google) and marketplace (Amazon).

See Perianne Boring, The Beauty Of The Blockchain, FORBES (Jun. 17, 2016),
This Note proceeds in three parts. Part I identifies the tripartite characteristics of Bitcoin: the blockchain, the protocol, and the currency. It examines the processes within the Bitcoin ecosystem and demonstrates how a bitcoin transaction operates and explains the layout of the blockchain ecosystem in terms of the transaction, recording, and verification. Part II addresses how blockchain technology will disrupt the financial services industry. First, it addresses the digitization of the banking industry. Second, it identifies the need for collaboration between banks and FinTechs. It explores what precautions need to be taken to ensure consumer protection and security of one’s digital identity and why it is in the government’s best interest to endorse blockchain technology. Third, it examines the regulatory challenges that banks and FinTechs face prior to the implementation and widespread adoption of blockchain technology can take place. Part III evaluates the legal and regulatory issues that may arise as a result of blockchain’s disruptive role in the financial services industry. First, it identifies the current state of regulation for the application of distributed ledger technology as a virtual currency. Second, it analyzes how a disjointed regulatory emphasis on virtual currencies and failure to endorse blockchain technology in the financial services industry directly threatens to stifle innovation, capital formation, consumer protection, and national cybersecurity. Third, it compares the rules-based regulatory approach to money licensing regimes in the United States with the United Kingdom’s principles-based regulatory sandbox. Fourth, it argues why a national FinTech charter would be possible to implement in the United States and how it would correspond with joint proposed rule by the Office of the Comptroller, Department of Treasury and Federal Deposit Insurance Corporation for cybersecurity standards.

I. IT’S ALL ABOUT THE BLOCKCHAIN

Bitcoin is the first and largest cryptocurrency.\textsuperscript{43} A cryptocurrency is a peer-to-peer ("P2P") version of electronic cash that allows payments to be sent directly from one party to another without the need of an intermediary.\textsuperscript{44} There are three phases of the global financial technological revolution: Blockchain 1.0 emphasizes virtual currency,\textsuperscript{45} Blockchain 2.0 isolates technology and pro-
Protocol applications as to contracts,46 and Blockchain 3.0 is the expansion of the technological applications beyond finance and markets.47 This Note is limited to addressing the transition between Blockchain 1.0 to Blockchain 2.0. First, this Section answers the question, “What is the difference between bitcoin and blockchain?” by explaining the properties of the blockchain ecosystem. It accentuates the special properties of this technology and how it can be applied in the financial services industry. Finally, it analyzes why the application of blockchain technology will disrupt the financial services industry.

A. Bitcoin Ecosystem: Blockchain, Protocol, and Currency

Blockchain technology enables secure electronic transactions of bitcoin through the Bitcoin protocol, which employs cryptography to validate transactions before recording them on a decentralized48 public ledger.49 The ledger in which all network transactions are displayed is the blockchain.50 Bitcoin is trustless technology51 that exists through a decentralized peer-to-peer (“P2P”)52 consensus network of Bitcoin clients (also known as nodes).53 The Bitcoin pro-

46 Id. Blockchain 2.0 space can include Bitcoin 2.0 protocols, smart contracts, smart property, Dapps (decentralized applications), DAOs (decentralized autonomous organizations), and DACs (decentralized autonomous corporations). Melanie Swan, Decentralized Money: Bitcoin 1.0, 2.0, and 3.0, INSTITUTE FOR ETHICS AND EMERGING TECHNOLOGIES (Nov. 10, 2014), http://ieet.org/index.php/IEET/more/swan20141110.

47 See id.

48 GARETH W. PETERS AND EFSTATHIOS PANAYI, UNDERSTANDING MODERN BANKING LEDGERS THROUGH BLOCKCHAIN TECHNOLOGIES: FUTURE OF TRANSACTION PROCESSING AND SMART CONTRACTS ON THE INTERNET OF MONEY 4 (2015). “Decentralization” describes conditions under which the actions of many agents cohere and are effective despite the fact that they do not rely on reducing the number of people whose will counts to direct effective action.

49 Id. at 3-4. The word “ledger” refers to a book or set of records.

50 Id. at 4; see also Bruno Campenon, Fintech and the future of securities services, 8 J. SEC. OPERATIONS & CUSTODY 107, 111 (2016) (“[B]itcoin acts as a decentrali[z]ed depositary, messaging system and settlement platform rolled into one.”)


52 A P2P network is a “network of personal computers, each of which acts as both client and server, so that each can exchange files . . . with every other computer on the network.” Peer-to-peer Network Definition, DICTIONARY.COM, http://dictionary.reference.com/browse/peer-to-peer%20network (last visited Sept. 30, 2016).

Protocol employs public-key cryptography to verify and secure bitcoin transactions. As a publically distributed ledger, the blockchain ensures that all computers in the “Bitcoin network” have an updated and verified record of transactions within the network. Thus, the transparent nature of transactions in the Bitcoin network that are recorded on the blockchain prevents fraud and the “double-spending” problem by ensuring that every cryptocurrency can be spent only once.

1. Public Cryptographic Key

Bitcoin’s decentralized public ledger is the blockchain. The blockchain is a “chronological database” of all transactions that have been validated by network both provide and consume services at the same time with reciprocity acting as the incentive for participation.”).


Satoshi Nakamoto, BITCOIN: A PRIMER FOR POLICYMAKERS 7 (2nd ed. 2016) (detailing the life cycle of a bitcoin transaction).

The double spending problem is also called the “Byzantine Generals problem” – generals who are circling the enemy need to either simultaneously launch their attack or retreat; some attackers may be traitors, spread misinformation and effectively foil the attack. See Leslie Lamert et al., THE BYZANTINE GENERALS PROBLEM, 4 ACM Transactions on Programming Languages and Systems 382-401 (1982) (addressing reliability concerns computer communications). Satoshi Nakamoto’s “Bitcoin solution” to this Byzantine Generals Problem cannot be understated – it is simply revolutionary.” KELLY, supra note 18, at 57.

Andrews M. Antonopoulos, MASTERING BITCOIN, LOC. Chapter 1 (2015) (ebook), http://chimera.labs.oreilly.com/books/1234000001802/index.html. See also Kuo Chuen, supra note 44, at 12 (detailing the technical aspects of a bitcoin transaction). See generally KELLY, supra note 18, at 23 (earliest known banking ledgers date to 9000 BCE when transactions were literally written in stone).

See also Paul H. Farmer, Jr., Note & Comment, Speculative Tech: The Bitcoin Legal Quagmire & the Need for Legal Innovation, 9 J. Bus. & Tech. L. 85, 88–89 (2014) (“The Bitcoin peer-to-peer network that allows for miners to generate Bitcoins also serves as a public ledger for all Bitcoin transactions . . . The full record of transactions [within the network] is called a block chain, a sequence of records composing a virtual ledger.” (footnotes omitted)).

Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, SSRN 6 (Mar. 10, 2015),
Bitcoin network participants. Each block that is added onto the blockchain represents a transaction between two network users that manifested their intent to transact by exchanging a minimum amount of public information, and is verified by network participants, who compete to decrypt the puzzle of transaction consisting of private information. Once computers in the network reach a consensus on the transaction’s validity, it is recorded and timestamped as a new block on blockchain.

Network users are given one public key, also known as a “public address” that is shared to the network, like a social media profile page, and one private key, the content of which is kept secret, like a password. The address informs network participants where to transfer value.

In order for bitcoin transactions between Bitcoin network users to appear on the blockchain, parties must first manifest their intent to transact through the exchange of their public key. In a bitcoin transaction, an individual proves authentication of bitcoin ownership through their private key and transfers the value to the new owner’s address through the public key. Transactional secure...


62 Kuo Chuen, supra note 44, at 16.

63 Blockchain, Bitc... (last visited Oct. 31, 2016), (providing that “[a] block chain is a transaction database shared by all nodes” on a network).

64 Mining Bitcoin Has Become A Ruthlessly Competitive Business, BUSINESS INSIDER (Jan. 11, 2015), http://www.businessinsider.com/mining-bitcoin-is-a-competitive-business-2015-1 (providing that the cryptography competition ends when one node decrypts the transacting parties puzzle—the decrypted puzzle verifies that the public identify of the parties corresponds with private information of the deal, namely the sufficiency of funds between the parties which underlies the parties transaction); JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 8 (2nd ed. 2016 (explaining that mining involves the search is to find a sequence of data that produces a particular pattern when the Bitcoin “hash” algorithm is applied to the data”).


67 Bitcoin uses the public-cryptographic keys to maintain the “creation, use, and transfer of digital value.” KEVIN C. TAYLOR, FINTECH LAW: A GUIDE TO TECHNOLOGY LAW IN THE FINANCIAL SERVICES INDUSTRY 12-2 (2014).

68 JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 7 (2nd ed. 2016) (detailing the life cycle of a bitcoin transaction).


ty on the blockchain is afforded through the combination of a cryptographic hash. Bitcoin solves the double-spending problem and provides transactional security wherein each transaction has a digital signature and contains a cryptographic hash that allows for easy tamper detection. Thus, the two parties’ exchange of public keys initiates a bitcoin transaction because it effectively requests computers on Bitcoin Network to validate the transaction to decrypt, through the public key’s information, the content of the private.

2. Blockchain Protocol and Consensus-Based Transaction Mechanisms

Consensus

Bitcoin exists through a peer-to-peer network (“P2P”) of Bitcoin users who have access to all transactions. As a distributed public ledger, Bitcoin requires that all transactions be publically announced to all computers on the Bitcoin network, called nodes. If Alice wants to transact with Bob, Alice initiates this process by broadcasting to the network “I, Alice, give Bob one bitcoin” by signing off the transaction with her private key (i.e., her signature). Before Bitcoin network users can view transactions on the blockchain ledger, miners must first reach a consensus to validate the transaction. Users that providing

71 See Peters & Panayi, supra note 66, at 243.
72 See Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, BITCOIN (2009), https://bitcoin.org/bitcoin.pdf. See also Peters & Panayi, supra note 66, at 243 (evaluating how second-generation contract-based developments of blockchain technology can be applied to data integrity protocols in the banking industry to achieve varying degrees of “permissioning, data integrity, and data security.”).
73 Kuo Chuen, supra note 44, at 16.
75 Peer-to-peer Network Definition, DICTIONARY.COM, http://dictionary.reference.com/browse/peer-to-peer%20network (last visited Feb. 10, 2017) (a P2P network is a “network of personal computers, each of which acts as both client and server, so that each can exchange files... with every other computer on the network”).
76 Private or permissioned blockchains are also known as shared or distributed ledgers. Gideon Greenspan, Payment and Exchange Transactions in Shared Ledgers, 10 J. Payments Strategy & Sys. 172, 172 (2016) (identifying what characteristics distinguish distributed ledgers from centralized ledgers, as well as bitcoin-style blockchain from ethereum-style blockchain).
computing power to log and reconcile transactions on the ledger are called *miners*. Miners compete to be the first to validate the transaction through computationally intense process, known as “proof-of-work,” in which they determine the legitimacy of the transaction. Once a consensus has been reached as to the transaction’s legitimacy, it is recorded, time-stamped, and displayed in one “block” of the blockchain.

3. Proof of Work

A “block” of data will be added to the blockchain once computers on the Bitcoin network reach a consensus as to the transaction’s validity. The mechanism in which transactions are validated is through the computationally intensive “proof-of-work” of all transactions that constitute the blockchain and depends upon the amount of computing processing power being contributed to the network. Mining is integral in the issuance of new bitcoins and is a necessary process for transactions to be added onto the blockchain and subsequently verified. The mining process in which transactions are verified is computationally intensive to ensure that only legitimate transactions are verified and recorded onto the blockchain.

B. The Evolution of Financial Intermediaries and the Application of
Blockchain Technology

The distributed ledger technology of Bitcoin’s blockchain can virtually incorporate the contractual process in “anything that can be digitally identified.” Consequently, blockchain technology enables the creation and execution of digital “smart contracts,” a term Nick Szabo first introduced in 1996. The development of FinTech, blockchain technology, and associated smart contracts, has the potential to reshape transaction costs in the financial system. It is significant to note, however, that smart contracts are automation, not law. Smart contracts are modules of computer code that are dependent on certain triggering conditions to transfer digital assets on the blockchain. Smart contract protocol can specify, as computer code, the terms under which certain obligations are fulfilled and can execute actions like sending a payment or deactivating a file once there is evidence of the contract’s terms’ fulfillment.

The evolution of financial institutions is arguably shaped by the relationship between varying levels of trust and differences in transaction costs. Specifically, it is argued that the application of distributed ledger technology will disrupt traditional financial service institutions because it revolutionizes the role of the

89 Kelly, supra note 18, at 153.
91 See Michael Gord, Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality, Bitcoin Magazine (Apr. 26, 2016), https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/ (conceiving the idea of digital “smart” contracts); but see Allan I. Mendelowitz & Willi Brammertz, Smart Contracts Were Around Long Before Cryptocurrency, Am. Banker (Nov. 17, 2016), http://www.americanbanker.com/bankthink/smart-contracts-were-around-long-before-cryptocurrency-1092463-1.html (noting that banks have imperfectly implemented smart contracts into their business for three decades, as exemplified by transaction processing systems and data warehouses).
93 See Id: Kelly, supra note 18, at 150 (identifying smart contracts as legal documents attached to a bitcoin transaction).
94 Permissioned, in this context, means shared among the parties involved in a transaction.
95 Hazard et al., supra note 92, at 225.
intermediary. The three dimensions of transaction costs, which are (1) definition and manufacturing, (2) monitoring, and (3) enforcement of contracts, resemble the stages of financial banking intermediation, which involve (1) underwriting and manufacturing of financial instruments, (2) monitoring and screening credit and market risks to the value of contracts, and (3) enforcement/execution of financial contracts. Banks’ business model of operating through the centralization of control has not significantly changed from Italian banks of the 1400’s and commercial banks of the 1930’s. However, the geographical expansion of what diverse and complex services and transactions banks could provide clients has resulted in the association of financial intermediaries with an increase in transaction costs. Blockchain technology, therefore, has been recognized as the most “truly disruptive technological advancements to the practice of law since the invention of the printing press” because smart contracts can facilitate the replacement of banking financial intermediaries. The role of banks in intermediation, initially established to solidify trust among contract counterparties and promote transparency, depreciates in the presence of a trustless technology that accomplishes the same functions.

A smart contract is self-executing software that is able to autonomously and precisely determine each payment required by the contract. To be put differently, a smart financial contract represents the black-letter legal obligations contained in a natural language contract. The risks posed by smart contracts are reduced because they are autonomous, self-sufficient, and decentralized. Smart contracts resemble the design of Bitcoin in that they “subsist inde-
pendently of any moral or legal entity.”¹⁰⁵ Smart contract codes define and manage ownership rights.¹⁰⁶ Due to the immutability of a decentralized and distributed ledger, the smart contract codes do not make any assumptions about the assignment of rights, nor can they arbitrarily seize, divest or transfer these rights.¹⁰⁷ Smart contract code is jurisdictionally neutral and therefore allows “borderless” enforceability, no longer restricted by the jurisprudential reliance of political borders. With smart contracts, it is the code that is the law.¹⁰⁸ As a result, the trustless blockchain provides a faster, more efficient, and secure means of transacting and contracting, and the reduction of transaction costs will increase the amount of market participants.

In conclusion, decentralized and autonomous applications of blockchain will disrupt the traditional role of intermediaries. The implementation of smart financial contracts in an open source dynamic will result in the optimization of contracting and transacting. The impact of distributed ledger technology and the application of smart contracts in the financial services industry will be discussed in the next Section.

II. DISRUPTION: THE ROLE OF FINTECH SERVICES IN TRADITIONAL BANKING

The disruptive role that blockchain will have on banking is clear – banking financial intermediaries operate through a centralized control of authority and the autonomous, self-serving, and decentralized applications of blockchain replace the intermediaries.¹⁰⁹ This section analyzes how blockchain technology will disrupt the financial services and banking industry. It emphasizes the economics of blockchain in terms of how disintermediation¹¹⁰ and decentralization will likely shift the economic organization of banking.¹¹¹

¹⁰⁶ See Tapscott & Tapscott, supra note 38, at 142 (explaining how smart contracts eliminate the need for a bureaucracy to define ownership and generate wealth).
¹⁰⁷ Id. at 143 (2016) (describing how the functionality of the code would replace the need for a centralized ledger).
¹⁰⁸ See Lawrence Lessig, Code Version 2.0 4 (2d ed. 2006) (arguing “[c]ode is law” and that within the realm of cyberspace, the invisible hand, pushed by government and by commerce, highly efficient regulation is possible).
¹⁰⁹ See generally Sundararajan, supra note 97, at 93.
¹¹¹ Trent J. MacDonald, et al., Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking, in Banking Beyond
A. Why the Financial Services Industry is Ripe for Disruption

The general function of blockchain technology is that it eliminates the role of a financial intermediary. Thus, financial services is the most “obvious industry” for initial “blockchain marketplace development” and disruption for a number of reasons. Consider the three factors that define a bank: (1) by its legal form; (2) by the services it offers; and (3) economic function to society. Its economic function to society is categorized by its role in financial intermediation and transaction services. Banks have dominated the payment system. Historically, a common feature of payment systems was that payment service providers, traditionally banks, were at the same time standard-setters and owners of the infrastructure.

Traditional legacy bank structures continue to dominate. Card networks, money transmissions and counterparty connectivity enable banks, merchants, and owners of the infrastructure.

Banks and Money 279, 284 (Paolo Tasca et al., eds., 2016).

112 Kelly, supra note 18, at 57.
113 Sundararajan, supra note 97, at 91.
115 Id. at 56-57 (quoting United States v. Phil. Nat’l Bank, 374 U.S. 321, 326 (1963) (“Banks are unique among financial institutions in that they are alone permitted by law to accept demand deposits. This distinctive power … gives banking a key role in the national economy. For banks do not merely deal in, but are actually a source of, money and credit…Furthermore, the power to accept demand deposits makes banks the intermediaries in most financial transactions (since transfers of substantial moneys are almost always by check rather than by cash) and concomitantly, the repositories of very substantial individual and corporate money. The banks use this money is conditioned by the fact that their working capital consists largely of demand deposits, which makes liquidity the guiding principle of bank lending and investing policies; this it is that banks are the chief source of the country’s short-term business credit)).
116 Id. at 38-46 (emphasis in original).
117 Id. at 39-40 (explaining that the benefits that financial intermediaries provide include (1) offering diversification, (2) enable investors to enjoy economies of scale, (3) offer expertise, (4) convert illiquid investments into liquid ones).
118 Id. at 39-40.
119 Id. at 54 (5th ed. 2013).
122 For example, the Visa, MasterCard, SWIFT, EBA, CHIPS, Fedwire, RTGS, and ACH, all of which have a relationship with traditional banking, dominate the market. Chris Skinner, ValueWeb: How Fintech Firms are Using Bitcoin Blockchain and Mobile Technologies to Create the Internet of Value 155 (2016).
corporates, and institutions to interoperate with trust and security. However, as a consequence of the technological revolution, banks’ monopoly position as a payment services provider has been jeopardized by FinTechs that target “narrow financial services.” The goal of these narrow financial services is the unbundling of banking through the offering of banking components.

Looking at the evolution of the banking technology in the United States, disintermediation and the concept of digitalization being disruptive are not new. What is revolutionary, however, is that the blockchain democratizes value in the same way the Internet of Things democratized information.

---


124 Miller & Cafaggi, supra note 121, at 119.

125 See Skinner, supra note 123, at 13 (discussing how technology is changing the structures built in the past for paper distribution).

126 See id. For example, the peer-to-peer payment application Venmo, owned by PayPal, provides an instantaneous monetary-transfer service. See e.g., Steve Lohr, A Financial Industry Scramble As More Pay by Smartphone, N.Y. TIMES, Jan. 19, 2016, at A-1 (recognizing that the millennial-led shift toward digital financial services, like Venmo, threatens to permanently depriving to permanently deprive the consumer banking industry of one of its sectors).


128 The removal of intermediaries is not a revolutionary concept, or one that banks are unfamiliar, given the expansion of the computer placed mainframe computing power on the desktop for personal use and the personalization of online banking, made possible by the Internet. Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, SSRN 48-49 (Mar. 12, 2015) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

129 See Sundararajan, supra note 97, at 54-56 (discussing how digital forces sustained crowd-based capitalism); see also Skinner, supra note 123, at 159; see also Joseph L. Bower & Clayton M. Christensen, Disruptive Technologies: Catching the Wave, HARV. BUS. R. (1995), https://hbr.org/1995/01/disruptive-technologies-catching-the-wave (recognizing that one of the determinative factors that contributes to a business’s failure, success, or market domination is its ability to develop and commercialize new technologies that adequately address the next-generation performance needs of their customers).

130 Tapscott & Tapscott, supra note 38, at 299.
Blockchain operates a decentralized public ledger of transactions that no one person or company owns or controls. In the “Internet of Value” the blockchain is referred to as the “value exchange network” because it is an exchange platform for digital value on the Internet and the programmability of its bitcoin has the ability to trigger efficient, fast, and secure actions directly wired into the real world. Similar to how the Internet of Things fundamentally changed the way we share information, blockchain is an open source innovation that is going to revolutionize the transactions amongst individuals, governments, businesses, and machines.

As a part of the P2P sharing economy, the role of banks has expanded from profit and trade to include community and social interaction. In an effort to

131 See Yochai Benkler, The Wealth of Networks 62 (2006) (defining democratization as “conditions under which the actions of many agents cohere and are effective despite the fact that they do not rely on reducing the number of people whose will counts to direct effective action”).

132 Mihaela Ulieru, Blockchain: what it is, how it really can change the world, WORLD ECONOMIC FORUM (June 23, 2016), https://www.weforum.org/agenda/2016/06/the-blockchain (last visited Sept. 24, 2016); see also William Mougayar, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology 90 (2016); see also Craig K. Elwell et al., CONG. RESEARCH SERV., R43339, Bitcoin: Questions, Answers, and Analysis of Legal Issues 1, 6 (2015).

133 See Sundararajan, supra note 97, at 56 (noting that the Internet of Things is transitioning from the early internet’s consumerization of the digital and onto the digitalization of the physical).

134 See Mougayar, supra note 132, at 155 (giving an example, that trust components are stored on the blockchain (identity, rights, membership, ownership, and time stamping), services where a contractual component is executed on the blockchain (proof of service and proof of compliance), on decentralized peer-to-peer market (e.g., OpenBazaar or La’Zooz), through a Distributed Autonomous Organization (whose governance and operations run on the blockchain)).

135 Perianne Boring, The Beauty Of The Blockchain, FORBES (June 17, 2016), http://www.forbes.com/sites/perianneboring/2016/06/17/the-beauty-of-the-blockchain/#2bf379194489; see also Jacob Morgan, A Simple Explanation Of The Internet Of Things, FORBES (May 13, 2014), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1b4567d46828 (defining the Internet of Things as “the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other)”).


138 See Skinner, supra note 123, at 77 (discussing how banks are adapting to mobile opportunities). There are three categories of start-applications: wrappers, replacers, and
maintain and acquire customers that prioritize the digital components of banking, banks have been leading in the market of mobile innovation.\textsuperscript{139} The increase of startup banking applications which merely “wrap” themselves around a bank’s mobile ecosystem do not pose a threat to the bank’s own innovations.\textsuperscript{140} However, given the rate at which technological payment innovations have moved from mobile and onto taking payments in “connected ‘internet of things’ devices,” the traditional payment infrastructure has struggled to keep up.\textsuperscript{141} This shortcoming reveals a differential feature between banks’ and FinTechs\textsuperscript{142} respective market advantages and institutional strengths: whereas banks’ stop-gap strategy has been to layer new technological solutions on top of legacy systems, FinTechs are already digital at their core.\textsuperscript{143} Notably, banks and FinTechs each possess something that the other is likely unable to acquire within the immediate future: banks have the market expertise, regulatory familiarity, trusted brand name, and most importantly, a banking license, and FinTechs innovate with digital embedded in their culture.\textsuperscript{144}

\textsuperscript{139} See id; see also \textit{Episode #134: Blockchain is essential to the Fintech revolution}, SoundCloud: BreakingBank$ (Mar. 3, 2016) available at https://soundcloud.com/breakingbanks/blockchain-essential-fintech (recognizing that the “digital” consumer no longer evaluates their satisfaction with banks according to a standard of friendliness).

\textsuperscript{140} See \textit{Skierner, supra} note 123, at 228 (proposing that human behavior will forward the next technological issues of the future).

\textsuperscript{141} Hannah Kuchler, \textit{Payments networks battle new breed of criminals in cyber attacks}, \textit{FIN. TIMES} (Sept. 28, 2016), https://www.ft.com/content/44340cda-4ff5-11e6-8172-e39ed3b86fc (providing that banks in competition with fintechs must perform cost benefit analysis to determine whether the risk of fraud outweighs a less convenient user experience).

\textsuperscript{142} The label “fintech” may be affixed “to almost any start-up that is trying to use technology to solve some financial problem, and that can mean everything from insurance brokering to data analytics to budgeting software.” \textit{Ranking the Top Fintech Companies, N.Y. TIMES} (Apr. 6, 2016), http://www.nytimes.com/interactive/2016/04/07/business/dealbook/The-Fintech-Power-Grab.html?_r=0; FinTech is comprised of five areas: (1) finance/investment, (2) operations/risk management, (3) payments/infrastructure, (4) data security monetization and (5) customer interface. See \textit{Douglas W. Arner et al., The Evolution of FinTech: A New Post-Crisis Paradigm?} 18 (2015) (unpublished manuscript) (on file with the University of New South Wales Law Research Series) available at http://ssrn.com/abstract=2676553.

\textsuperscript{143} See \textit{Skierner, supra} note 123, at 227 (discussing the emergence of Banco Original in Brazil); see also Robert Barba, \textit{B of A’s Bessant on AI, Blockchain, Patents and Swift}, \textit{AM. BANKER} (June 8, 2016) http://www.americanbanker.com/news/bank-technology/b-of-as-bessant-on-at-blockchain-patents-and-swift-1081389-1.html (noting banks that use technology cannot afford to be pure fintech companies because customers have much higher expectations of reliability).

\textsuperscript{144} See \textit{Skierner, supra} note 123, at 229-231(discussing the difference between tradition-
The proliferation of smartphones has resulted in a rapid increase in the growth of “mobile wallets,” which enable consumers to make payments via their mobile phones. Despite millennial assertions that privacy is a priority, the relinquishment of their private data to third parties suggests the significance of the need to enhance privacy protections to safeguard personal identity information stored in digital wallets. Any device that has an IP address and is connected to the Internet of Things is a vulnerability. When considering the type and value of data secured by banks that is made accessible to its customers through the Internet, potential unknown vulnerabilities in current mobile banking software risk open source software breaches. With the understanding that payment systems are only as trustworthy as their weakest link, the message to central banks and FinTechs alike is if you can’t beat them, join a consortium.

145 See, e.g., Erin F. Fonté, Mobile Payments in the United States: How Disintermediation May Affect Delivery of Payment Functions, Financial Inclusion and Anti-Money Laundering Issues, 8 WASH. J. L. TECH. & ARTS 419, 421-22 (2013) (“Mobile payments technology is poised to create a globally dramatic shift in how individuals pay for goods and services, track spending, and manage personal finances.”).

146 BNY MELLON, INNOVATION IN PAYMENTS: THE FUTURE IS FINTECH 1 (2015), https://www.bnymellon.com/_global-assets/pdf/our-thinking/innovation-in-payments-the-future-is-fintech.pdf (acknowledging that the “era of fintech” is before us and bank’s mindfulness is insufficient; banks must establish a clear plan “to adapt to and benefit from fintech-fuelled changes.”).


149 See id.

150 See id.

151 See id (acknowledging that “[p]eople have become a little too cavalier about internet-connected devices.”).


153 See Jane Wild, Central banks explore blockchain to create digital currencies, WALL ST. J. (Nov. 2, 2016), https://www.ft.com/content/f15d3ab6-750d-11e6-bf48-b372cdb1043a (recognizing that as worldwide central bank experimentation with blockchain progresses, cross-border cooperation will be necessary to address regulating developments in digital currency).
B. How Will Blockchain Technology Change Financial Institutions

The FinTech competition to incorporate distributed ledger technology into the financial services industry has gone global. To date, the greatest challenge that FinTech companies face in developing what will comprise the new core of the blockchain banking industry is developing a ledger that properly balances transparency to financial markets with protecting consumers’ financial and identity information. In attempting to achieve this balance, the crux of the competition, that divides FinTech and blockchain banking initiatives alike, is whether the best interests of the industry will be served/achieved through a permissionless, distributed public ledger or a permissioned, distributed private ledger.

Distinguishable from Bitcoin’s permissionless, or public, blockchain that enables a universal market to access to all information, “permissioned,” or private, blockchains are those in which only known, trusted entities can participate. Through a permissioned distributed ledger, sensitive information would never be published. It is highly likely that more financial institutions will opt for a permissioned distributed ledger that will limit the sharing of information

---


155 The notable banking blockchain competitors include R3, Symbiont, Digital Asset Holdings, and CitiGroup. Compare Digital Asset Holdings’ private distributed ledger model which is anchored in a “need-to-know” basis model (“Shared ledgers should contain the bare minimum information, interpretable only by those with a need and right to know, to permit notification, synchronization and confirmation.”) with Symbiont. Tanaya Macheel, Banks’ Privacy Concerns Shaping Blockchain Vendors’ Strategies, AM. BANKER (July 26, 2016), http://www.americanbanker.com/news/bank-technology/banks-privacy-concerns-shaping-blockchain-vendors-strategies-1090411-1.html.

156 As an open source innovation for financial disintermediation, the Bitcoin blockchain was designed with an “all or nothing” approach to transact, validate and access transactions publically. The sensitive information should never be published; some say all data should be published, even if some of it must be concealed. Addleshaw Goddard LLP, Blockchain – Public or Private, LEXOLOGY (Nov. 17, 2016), http://www.lexology.com/library/detail.aspx?g=a381bb8a-3494-48d-9655-7f469efdd23.

157 See Gideon Greenspan, Payment and Exchange Transactions in Shared Ledgers, 10 J. PAYMENTS STRATEGY & SYS. 172, 172-77 (2016) (identifying what characteristics distinguish distributed ledgers from centralized ledgers, as well as Bitcoin-style blockchain from Ethereum-style blockchain).

158 For a more technical understanding of the difference between permissioned and permissionless ledgers, see Tim Swanson, Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems 5 (2015).

with the parties on a need-to-know basis while improving upon the quality of the consumer, business, or regulatory relationship. As financial institutions incorporate distributed ledger technology, a balance must be struck between maximizing efficiency and minimizing transaction costs, without sacrificing market stability, and consumer protection must take into consideration how cybersecurity risks will be mitigated.\(^\text{160}\)

C. Advantages of Incorporating Blockchain Technology in Banks

The primary characteristics of distributed ledger technology are its immutability, transparency, and autonomy.\(^\text{161}\) The autonomous execution capabilities of blockchain technology – both FinTech and regulatory technology (“Reg-Tech”) would enable compartmentalized access to financial information that provides immutable and real-time updates that facilitate automated review. Blockchain technologies have the potential to transform financial and industrial markets, challenge corporate boundaries,\(^\text{162}\) and add transparency to the public sector.\(^\text{163}\) The benefits of blockchain technology include reduction in transaction costs,\(^\text{164}\) increase in regulatory compliance, instantaneous settlement,
increased security, and streamlined international trade finance through global interoperability. To date, the areas in which DLT is thought to be most impactful include the financial markets in payments, banking, securities settlement, and the trade of digital and financial assets. Accordingly, the advantages of incorporating blockchain technology as it applies to regulatory compliance functions include: compliance software that utilizes artificial intelligence to monitor trading activity by automatically learning patterns to detect illegal activity; recording derivative trades; monitoring the risk national banks are exposed; and programming mobile applications to notify and report suspicious account activity to bank managers in real-time. As a consequence, traditional legacy banks will experience fundamental shifts in their organizational boundaries, with many transactions currently governed through hierarchy, relational contracting, or market transactions that will shift to the blockchain as an outworking of economic efficiency over transaction costs.

The political economy of blockchains challenges the legacy of banking, financial organizations, and market structure. Blockchains are apt to outcompete hierarchical organizations such as banks, and relational market contracting, which are transactions requiring trust. Therefore, the redistribution of value amongst financial institutions that have or have not adapted to DLT will be inevitable, and consequently, will warrant the recalibration of banking as an institution. To date, a majority of financial institutions that are at the forefront of the global financial technological revolution are those Too-Big-To-Miss-Out — either, they were recognized as institutionally worthy enough to join a consortium or were capable of financing their own in-house FinTech

---

165 Tapscott & Tapscott, supra note 38, at 71.
166 Id.
168 See Melanie Swan, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY 15 (2015), http://w2.blockchain-tec.net/blockchain/blockchain-by-melanie-swan.pdf (“Blockchain based smart property contemplates the possibility of widespread decentralized trustless asset management systems as well as cryptographically activated assets.”); see also Sundararajan, supra note 97, at 91 (explaining that centralized institutions “increase costs, freezes innovative potential, and needs layers of reconciliation.” Adam Ludwin, CEO of Chain identified blockchain at the “new database technology, purpose-built for trading assets.”).
169 Diana C. Biggs, HOW NON-BANKS ARE BOOSTING FINANCIAL INCLUSION AND REMITTANCE, in BANKING BEYOND BANKS AND MONEY: A GUIDE TO BANKING SERVICES IN THE TWENTY-FIRST CENTURY 190 (Paolo Tasca et al. eds., 2016).
170 MacDonald et al., supra note 111, at 279.
171 Id.
172 Id.
experimentation.

Regardless of whether financial institutions adopt a permissioned or permissionless distributed ledger, a shared repository with real-time access to data will facilitate transparency between regulators and regulated entities. Reporting activities through smart contracts will enable the automation of compliance activities. In conclusion, the characteristics distributed ledger technology allows for the adaptability to a rapidly changing marketplace demands and enables efficient responsiveness to and growing regulatory constraints.

PART III: REGULATION

“You will not find a solution to political problems in cryptography.”

A. History of Federal Regulation of Digital Currencies, Money Service Businesses, and Money Transmission in the United States

Regulators have chosen to regulate cryptocurrency businesses under the payments regulatory framework. Accordingly, the current regulatory approach to decentralized virtual currencies mirrors that of financial regulation in general, a hybrid of “ex ante and ex post regulation to mitigate systemic risk in the financial system.” This Section will outline the current regulations of virtual currency, the absence of legislation addressing distributed ledger technology, and the effect proposed cybersecurity standards will have on the future of global financial technology.

To date, the Department of the Treasury Financial Crimes Enforcement Network (“FinCEN”) and the New York Department of Financial Services (“NYDFS”) are the most notable examples of virtual currency proactive regulation. Under the Bank Secrecy Act (BSA), banks and other financial institutions are subject to various registration and recordkeeping requirements.

---

174 TAPSCOTT & TAPSCOTT, supra note 38, at 263.
and develop both anti-money-laundering and customer identification programs. In March 2013, FinCen issued guidance on the application of the Bank Secrecy Act and its implementing regulations to virtual currencies (“Virtual Currency Guidance”).

The Virtual Currency Guidance outlines the applicability of the existing federal anti-money laundering (AML) regime to convertible virtual currencies and includes decentralized virtual currencies. Virtual Currency Guidance thereby declared that “exchangers” and “administrators” of such currencies are subject to the AML requirements to the extent that they transmit decentralized virtual currency or legal tender from one user to another, or from one location to another. Additionally, it concluded that although a “virtual currency” would not be deemed a “currency” under regulations implementing the BSA, certain virtual currency businesses would nevertheless be money transmitters under the BSA, subject to regulation as money services businesses (“MSB”).

In 2014, FinCen attempted to clarify how the Virtual Currency Guidance applied to different decentralized technology business models and issued administrative guidance to address the regulation of virtual currency miners, soft-
ware development and investment activities, virtual currency trading platforms, and virtual currency payment systems. Despite FinCen’s numerous attempts to provide clarity in the scope of its guidance through administrative rulings, the significant risk of harm posed by ongoing issues vagueness and a lack of clarity is particularly problematic in the arena of digital currency innovations; the USA Patriot Act made noncompliance with state money license rules a federal crime whether or not a business is aware of the violation.

In June 2015, NYDFS promulgated its final “BitLicense” framework for regulating “virtual currency businesses.” Under NYDFS’s BitLicense framework, “virtual currency business activities” are categorized into five major prongs: (1) transmitting virtual currency; (2) holding virtual currency on behalf of others; (3) buying and selling virtual currency as a customer business; (4) providing exchange services as a customer business; and (5) controlling, administering, or issuing virtual currency. Distinguishable from NYDFS’s strict BitLicense regime, North Carolina is the only state that has proposed a bill that would adopt a lenient, regulatory sandbox approach to money transmitter licensing.

The Financial Stability Oversight Council (FSOC) was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). FSOC’s 2016 Annual Report acknowledged that “a considerable degree of coordination among regulators may be required to effectively identify


23 N.Y. COMP. CODES R. & REGS. § 200.02(o) (2015) (defining “transmitting virtual currency” as “the transfer, by or through a third party, of Virtual Currency from a Person to a Person.”).


See Hilary J. Allen, Putting the “Financial Stability” In Financial Stability Oversight Council, 76 Ohio St. L. J. 1087, 1088 (2015) (arguing that “both the FSOC’s structure and its mandate are flawed in ways that increase the susceptibility of financial stability regulation to the vagaries of political economy.”).
and address risks associated with distributed ledger systems.” 194 FSOC is the only agency that has a mandate to “identify risks to the financial stability of the United States” and to “respond to emerging threats to the stability of the United States financial system.” 195 Unfortunately, the effectiveness of the mandate is reduced because Dodd-Frank does not provide definition for the term “financial stability.”

B. The Repercussions of Deficient Regulatory Action Towards Blockchain Technology

Present alternative regulatory proposals primarily focus on “ex ante measures followed by ex post supplemental enforcement actions as necessary.” 196 Financial globalization establishes a “regulator[y] dilemma” for regulators who would like to benefit from international exchange but are wary of compromising their financial systems. 197 Accordingly, there is a gap in current distributed ledger technology policy recommendations between the policy concerns presently voiced by regulators and the frustration of many decentralized industry participants who want a limited national FinTechs charter.

Businesses that have monetary transmission licenses that even remotely engage with distributed ledger technology are potentially subject to federal monetary, anti-money laundering, investment, and consumer protection regimes, in addition to any of the 50 different state money transmitter licensing regimes in which their businesses engage. Federal authorities’ policy priorities have shifted from a concentrated focus on money-laundering, terrorist financing, and identity verification towards a more complex payments-related issues, including privacy and security, tax compliance, and the potential for use of unfair and deceptive businesses practices in the industry. 198 State regulatory activity also added new policy concerns to the mix, with a primary focus on consumer protection. 200

194 FINANCIAL STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT 127 (2016).
196 Reyes, supra note 176, at 221 (highlighting the “overwhelming[] emphasis on the payments applications of decentralized ledger technologies, curbing illicit uses of such payments applications, reducing the perceived extreme level of anonymity afforded to use of such payments applications, [and] protecting consumers from financial loss.”).
198 See generally CONF. OF STATE BANK SUPERVISORS, MODEL STATE CONSUMER AND INVESTOR GUIDANCE ON VIRTUAL CURRENCY 3 (Apr. 23, 2014), https://www.csbs.org/legislative/testimony/Documents/ModelConsumerGuidance—Virtual%20Currencies.pdf. See Reyes, supra note 176, 208 n. 96 (identifying the ten states that have released consumer guidance in accordance with the CSBS model).
199 Reyes, supra note 176, at 210.
200 Id.
Therefore, the Uniform Law Commission is working to draft the Virtual Currency Businesses Act. The Commission stated mission is to “harmonize” state-level regulation of virtual currencies “[i]n the absence of an overarching federal payments regulatory framework.” Due to the lack of clarity in FinCen digital currency regulations as it applies to distributed ledger technology, digital asset companies involved in MSB activities are being denied access to banking services without appropriate initial due diligence oriented towards understanding the actual business model. As a result of anti-money laundering, terrorist financing, and potential use for illicit-purposes risks that virtual currencies pose, licensed money transmitters are fearful that activities associated with blockchain distributed ledger technology will threaten their licenses and relationships with regulators. Besides being subject to disjointed federal and state money transmission and money services business regimes, entities engaged in transmitting money likely must comply with OFAC requirements, consumer protection obligations, as well as the CFPB’s Remittance Rule.

The trajectory of federal regulation of decentralized virtual currency is marked by an emphasis on ex ante attempts to prevent financial harm and ex post prosecutions of harmful activity that are a consequence of the former regulations’ incongruity with newly emerging technological applications. This has resulted in a financial technology “law lag,” which refers to the circumstances in which “existing legal provisions are inadequate to deal with a social, cultural or commercial context created by rapid advances in information and communication technology . . . .” By falling behind in the global financial

201 See generally Nat’l Conf. of Comm’rs on Unif. State Laws, Regulation of Virtual Currencies Act (draft), 6 (2015).
203 See Pratibha Vallabhani et al., Overcoming Obstacles to Banking Virtual Currency Businesses, Coin Center Report 11 (May 2016).
208 Electronic Fund Transfers (Regulation E), 12 C.F.R. § 1005 (2012).
209 Reyes, supra note 176, at 212.
technological revolution, overly broad regulations and vague administrative guidance that do not directly address blockchain technology stifle innovation, and economic growth will decrease financial institutional capabilities to combat cybersecurity threats.\textsuperscript{211} The OCC, CFTC, and SEC have been consistent in their acknowledgement of the potential of distributed ledger technology, their encouragement for collaboration between regulated financial institutions, and expression of caution to the operational and systematic risks posed by the new technology.\textsuperscript{212}

In conclusion, a lack of uniformity between states’ often vague and conflicting AML/BSA regimes, and the absence of a national limited FinTechs charter, have effectively stopped collaborative efforts between FinTechs and financial institutions. The absence of a national charter therefore jeopardizes American institutions’ relevance in the development of the future global financial system by creating an environment that is inhospitable to innovators. Given the absence of any incentives for banks to collaborate with FinTechs, it is arguable that there will be an increase in cybersecurity threats posed to financial institutions who do not update their cyber risk protocol. Thus, financial stability will not be attained under current virtual currency regulations and in turn, threatens the privacy of financial and personal identifiable information.

C. Comparing International Regulatory Actions Towards Payment Innovation

With the increased use of technology within the financial services industry, regulatory bodies have the opportunity to access a level of granularity in risk assessments that did not previously exist. The autonomous, self-sufficient, and decentralized nature of blockchain technology suggests that a rule-based, as opposed to principle-based, approach to regulation is better suited for blockchain technology because it would be difficult for computers to understand the nuances and spirit of the laws in which the rules have been promulgated.\textsuperscript{213} FinTech firms have suggested that the OCC create a limited purpose FinTechs charter \textsuperscript{214} that resembles the principles-based regulation of the United King-

\begin{footnotesize}
\begin{enumerate}
\item\textsuperscript{211} Hillary J. Allen, $\S=\$\textsuperscript{Bitcoin}\textsuperscript{?}\textsuperscript{,} $\textit{Suffolk U. Law School Research Paper No. 15-33}$ (May 18, 2016); Reyes, supra note 176, at 211.
\item\textsuperscript{212} Mary Jo White, Chairman, SEC, Opening Statements at the Fintech Forum (Nov. 14, 2016); Thomas J. Curry, Comptroller of the Currency, Remarks at the Chatham House ‘City Series’ Conference, “The Banking Revolution: Innovation, Regulation and Consumer Choice” (Nov. 3, 2016).
\item\textsuperscript{213} See Janos Barberis and Douglas W. Arner., FinTech in China: From Shadow Banking to P2P Lending, in \textit{Banking Beyond Banks and Money} 89-90 (Paolo Tasca et al. eds., 2016).
\end{enumerate}
\end{footnotesize}
dom and Japan that would provide FinTechs with a “passport” across several states. The OCC could create a risk-mitigating limited federal charter for FinTech firms which only authorizes FinTech firms to engage in some of the core activities of banks. Specifically, FinTech firms would possess the benefits of federal regulation, preemption of state law, and access to the payments system, but would not participate in risk-generating activities.

The United Kingdom’s financial regulatory system consists of the U.K.’s Financial Conduct Authority (“FCA”), Prudential Regulation Authority (“PRA”) and HM Treasury. In May 2016, the FCA launched Project Innovate, a regulatory sandbox for market entrants and incumbent financial institutions for the purpose of promoting competition through disruptive innovation to foster innovation in the U.K. financial services market. As a result of the U.K.’s principle-based approach to regulating payment innovations, it has experienced burgeoning success with payments experimentation and is “light-years ahead” of the United States in providing licensing options. In contrast with the United States’ state-by-state licensing regime, the European Union provides members with “passport regulation” which provides FinTech firms with licenses to make digital transfers across borders.

The eligibility criteria include the firm’s activity intent to be within the scope of FCA regulations, genuinely innovative product or service that provides a consumer benefit, genuine need for the sandbox, and preparedness for testing in a live environment. The U.K. has four levels of licensing for nonbank payments providers

---

215 See e.g., Telis Demos, Brexit Leaves Europe’s fintech Firms in the Lurch, WALL. ST. J. (June 27, 2016), https://www.wsj.com/articles/brexit-leaves-europes-fintech-firms-in-the-lurch-1467019802 (recognizing that if a FinTech firm is regulated in the United Kingdom’s FCA, it is regulated across the European Union).


217 Id.


221 See e.g., id. (recognizing that if a FinTech firm is regulated in the United Kingdom’s FCA, it is regulated across the European Union).

which adapt to the characteristics and business models of the requesting entity: (1) E-Money Institutions (“EMI”), (2) small EMI licenses, (3) Authorized Payment Institutions (“API”), and (4) small API licenses.223

The Office of the Comptroller of the Currency (OCC), released a white paper in March 2016 entitled “Supporting Responsible Innovation in the Federal Banking System.”224 In its paper, the OCC extended its support for innovation in the financial services industry that it views as “consistent with safety and soundness, compliant with applicable laws and regulations, and protective of consumer’s rights.”225 Additionally, it emphasizes the need to “support responsible innovation”226 and business cultures “receptive to responsible innovation.”227 In October 2016, the OCC issued that, as a part of its responsible innovation framework, it will establish the Office of Innovation to facilitate regulatory interagency coordination and serve as a technical assistance program for banks and non-banks.228 To date, the OCC has not yet decided to grant a national FinTech charter. However, Commissioner Thomas J. Curry of the OCC remarked in November 2016 that “if the OCC decides to grant a national charter …, the institution will be held to the same high standards of safety, soundness, and fairness that other federally chartered institutions must meet.”229 The Commissioner recognized that opposition to a limited purpose FinTech charter includes dispute over the scope of the charter, Congress being the more appropriate vessel to enact the charter, and concerns that states will be preempted from providing individualistic protections to its consumers.230 Correspondingly, Commissioner Curry asserted that while the OCC does have the authority to

225 Id.
226 Id.
230 Id.
issue a charter to companies that engage in at least one of three core banking functions—taking deposits, paying checks, or lending money – the OCC has never waived consumer protection compliance requirements because it does not have the authority to do so.

D. The Feasibility of a FinTech Federal Charter

The United States could substantially benefit from adopting a principles-based approach like the United Kingdom, especially considering recent regulatory developments that address the concerns addressed by opponents of the federal FinTech charter. The Federal Financial Institutions Examination Council (“FFIEC”) issued guidance regarding the risks and risk management practices that apply to the use of free and open source software (“FOSS”).231 The main risks that regulators identified include multiple risk management areas, including code customization, IT architecture, forking, systems integration and support, and legal risks.232 On October 25, 2016, FinCen released an advisory to assist financial institutions in understanding their BSA obligations regarding cyber-events and cyber-enabled crime.233 FinCen does not require financial institutions to report egregious, significant, or damaging cyber-events and cyber-enabled crime when such events and crime do not otherwise require the filing of a suspicious activity report (SAR).234 The guidance encouraged reporting SARs, collaboration between BSA/AML compliance and cybersecurity risk units, and the sharing of information between financial institutions to combat money laundering, terrorist financing and cyber-enabled crime.235

Banks’ information governance relates to data safeguards,236 record-keeping

232 Id. 233 FINCEN, FIN-2016-A005, Advisory to Financial Institutions on Cyber-Events and Cyber-enabled Crime (Oct. 25, 2016).
234 Id. 235 Id (identifying a “cyber-event” as [a]n attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information” and a “cyber-enabled crime” as “[i]llegal activities (e.g., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers).
236 The Gramm-Leach-Bliley Act (“GLBA”) applies to all financial institutions and governs the use, storage, and protection of personally identifiable information. Gramm-Leach-Bliley Act Pub. L. 106-102, 113 Stat. 1338, (codified in relevant part at 15 U.S.C. §§ 6801-6809 and §§ 6821-6837). Personally identifiable information is defined as: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information; ERIKA McCALLISTER ET AL., NIST GUIDE TO PROTECTING THE
requirements, and breaches of security information.\textsuperscript{237} While a financial institution may outsource the function to a service provider, it is unable to outsource its responsibility for compliance.\textsuperscript{238} The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency,\textsuperscript{239} and the Federal Deposit Insurance Corporation, have harmonized the principles articulated in the aforementioned FFIEC and FinCen releases, and proposed joint standards for enhanced cyber risk management standards for large and interconnected entities under their supervision and those entities’ service providers.\textsuperscript{240} The enhanced cyber risk management standards described in the ANPR would apply on an enterprise-wide basis to banking organizations and financial institutions with US$50 billion or more in total consolidated assets.

As technology dependence in the financial sector continues to grow, so do opportunities for high-impact technology failures and cyber-attacks. Due to the interconnectedness of the U.S. financial system, a cyber incident or failure of one entity may result in systemic consequences involving related entities.\textsuperscript{241} The agencies are considering implementing the enhanced standards in a tiered manner to imposing more stringent standards on the systems of those entities that are critical to the functioning of the financial sector. The proposed rule addresses five categories of cyber standards: cyber risk governance; cyber risk management; internal dependency management; external dependency management; and incident response, cyber resilience and situational awareness.\textsuperscript{242}

CONCLUSION

Distributed ledger technology will have the most disruptive impact on the financial services industry since the invention of the Internet. Banking consor-
tioms’ experimentation, development, and adoption of distributed ledger technology will substantially alter the intermediary roles of banks. Regulatory emphasis on the threat posed by virtual currencies, like bitcoin, has created an environment that is inhospitable to innovation. For the full potential of block-chain technology to become a reality, the OCC must create a limited national charter for FinTechs. Whether or not distributed ledger technology is endorsed within the next year or the next decade, the United States’ participation in the global financial technology revolution warrants increased cybersecurity risk management standards.