UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 23 | Issue 1 Article 9

3-1-2019

The Future of Blockchain: As Technology Spreads, it May Warrant More Privacy Protection for Information Stored with Blockchain

Ashley N. Longman

THE FUTURE OF BLOCKCHAIN: AS TECHNOLOGY SPREADS, IT MAY WARRANT MORE PRIVACY PROTECTION FOR INFORMATION STORED WITH BLOCKCHAIN

I. INTRODUCTION

There are approximately 22 million Bitcoin wallets set up across the globe.[1] However, the number of users has been predominantly left to guesswork because many users own multiple wallets and conduct transactions from different addresses to increase their privacy protection.[2] Privacy and anonymity are the predominant reasons blockchain was developed and gained popularity.[3] Perhaps without surprise, Bitcoin's creator has maintained his own mysterious, fantasy-esque anonymity since introducing the currency in 2008.[4] While the desire to learn the true identity of the mysterious genius launched a global witch-hunt,[5] users reveled in the benefits of speedier, more efficient transactions[6] made with the encrypted and decentralized ledger system referred to as blockchain.[7]

---

1. Alex Lielacher, *How Many People Use Bitcoin in 2018?*, BITCOIN MKT. J. (July 31, 2018, 8:00 AM), https://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/.

2. *Id.*

3. *See* Matt Lucas, *The difference between Bitcoin and blockchain for business*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (May 9, 2017), https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/ (explaining how blockchain first came in to existence as a solution to the desire to circumvent government controls through anonymity, security, and cutting out the intermediary).

4. Zoë Bernard, *Everything You Need to Know About Bitcoin, Its Mysterious Origins, and the Many Alleged Identities of its Creator*, BUS. INSIDER (Dec. 2, 2017, 11:00 AM), https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12.

5. *See id.* (explaining the background behind Bitcoin's creation and the mysterious, anonymous creator).

6. *See* Jay Clayton, *Statement on Cryptocurrencies and Initial Coin Offerings*, U.S. SEC. AND EXCHANGE COMMISSION (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11 (discussing the numerous benefits to blockchain in finance).

7. *See* Bernard, *supra* note 4 (providing the history and growth in popularity of Bitcoin).

Blockchain is difficult to regulate because it is so new and has a variety of applications.[8] Some applications include maintaining healthcare records, executing smart contracts,[9] providing greater security to the Internet of Things,[10] and eliminating foul-play in governmental elections.[11] Although many applications for blockchain exist, one application that has received recent attention from regulators is the facilitation of transactions in cryptocurrency.[12] While blockchain has been around for ten years,[13] it is still relatively new to lawmakers, and regulators are just beginning to grapple with how to approach it.[14]

This Note seeks to forecast a direction in which blockchain technology and privacy law could go and highlight the concerns that this future might bring. The analysis looks to the privacy carve-out in the Supreme Court case *Carpenter v. United States*[15] as a potential means for adding privacy protection to information stored in blockchain ledgers in the future.[16] Part II discusses the origins of privacy law and the

8. *See* Clayton, *supra* note 6 (explaining the SEC's agenda for blockchain and cryptocurrencies, and the struggles of implementing regulation).

9. A smart contract is a programmable way to make sure that if certain conditions are met, something agreed upon will happen. They automatically verify that the terms are met before performing the contract, without requiring humans to review any data. *See* MAD NETWORK, *Differentiating Between Privacy and Secrecy on the Blockchain*, BITCOIN MAG. https://bitcoinmagazine.com/articles/differentiating-between-privacy-and-secrecy-blockchain/.

10. The "Internet of Things" refers to any object that can connect to the internet and that object's ability to connect to other objects through the internet. For example, your car might be linked to your calendar and already know the best route to take to get to your meeting. If the traffic is heavy or you are running late, the car might send a text to the other parties to notify them. Using this connectedness, society can begin to build "smart cities" with automation of many day-to-day activities. This increases the need for cybersecurity, which blockchain can provide. *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#6115f4191d09.

11. *17 Blockchain Applications That Are Transforming Society*, BLOCKGEEKS (2018), https://blockgeeks.com/guides/blockchain-applications/ [hereinafter BLOCKGEEKS].

12. *Blockchain Regulation: Technology is Welcomed, Cryptocurrency Regulated*, INTELLECTSOFT (April 23, 2018), https://www.intellectsoft.net/blog/blockchain-government-regulation [hereinafter *Blockchain Regulation*].

13. Bernard, *supra* note 4.

14. *See Blockchain Regulation*, *supra* note 12 (discussing the current regulatory issues with blockchain).

15. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).

16. *See* Harry Sandick & George LoBiondo, *Carpenter v. United States: An Initial Assessment*, PRIVACY L. WATCH (BNA) No. 140 (July 20, 2018) (suggesting that courts may

background information that will be useful in understanding the holding of *Carpenter*.[17] Part III reviews the facts, outcome, and reasoning behind *Carpenter*, and how that affects privacy law as it currently stands.[18] Part IV explains the functionality and weighs the pros and cons of blockchain technology for various applications.[19] Part V lays out the current blockchain regulatory scheme, attempts to forecast the future of blockchain, and highlights issues to be considered if blockchain were to become as prevalent as cell site location information.[20] Part VI concludes this Note.[21]

II. WHAT INFORMATION IS PRIVATE, AND HOW DO WE PROTECT IT?

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[22] This right includes common-law interests in protection of property from trespass.[23] For example, in 1928 the Supreme Court held in *Olmstead v. United States*[24] that wiretapping of public phone lines on public streets was not a search because there was no entry of defendants' homes or offices.[25] Although the Court later overturned *Olmstead*,[26] the case is still used to reference the Court's original line of thought regarding privacy protection.[27]

Almost forty years later, the Supreme Court in *Katz v. United States* expanded privacy protection to more than just property, by ruling

---

extend privacy protections to other types of technological records that are similar to CSLI, such as blockchain).

17. *See infra* Part II.

18. *See infra* Part III.

19. *See infra* Part IV.

20. *See infra* Part V.

21. *See infra* Part VI.

22. U.S. CONST. amend. IV.

23. United States v. Jones, 565 U.S. 400, 405 (2012) (citing Kyllo v. United States, 533 U.S. 27, 31 (2001)).

24. Olmstead v. United States, 277 U.S. 438, 466 (1928).

25. *Jones*, 565 U.S. at 405 (citing Olmstead v. United States, 277 U.S. 438 (1928)).

26. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (overturning the *Olmstead* narrow view that there must be a physical trespass to a defendant's home or office for the exclusionary rule to apply).

27. *See Jones*, 565 U.S. at 408 (stating that the *Katz* test has "*added to*, not *substituted for*, the common-law trespassory test").

that the Fourth Amendment protects "people, not places."[28] *Katz* introduced "the Harlan Standard,"[29] an analysis from Justice Harlan's concurrence where he stated that a Fourth Amendment violation occurs when an officer violates a person's "reasonable expectation of privacy."[30] This expectation includes both a subjective expectation of privacy, where the defendant felt an actual expectation of privacy, and an objective expectation of privacy, where society can agree that the expectation was reasonable.[31] The notion of a reasonable expectation of privacy can be shaped by multiple influences outside of the Fourth Amendment, such as property law and societal understandings.[32]

Generally, there has been an exception to the Harlan Standard when the information was stored by third-parties.[33] For example, the Supreme Court in *United States v. Miller* held that a bank depositor assumes the risk that his information may be revealed to the government by sharing that information with a third-party.[34] However, as technology advanced, courts and legislators continued to limit this third-party doctrine in favor of greater privacy protection, especially for financial records stored by third-parties.[35] The protection for financial information is a narrow one, given that disclosure is sometimes necessary and recordkeeping requirements are constitutional.[36] However, access to financial records must remain under the control of existing legal process.[37]

In 1976, the existing legal process relied heavily on property law concepts of ownership and possession in determining whether information stored by third-parties was constitutionally protected from a search without a warrant.[38] The Supreme Court concluded that where

28. *Jones*, 565 U.S. at 406 (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

29. *Id.*

30. *Id.* (citing Katz v. United States, 389 U.S. 347, 360 (1967)).

31. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

32. *Jones*, 565 U.S. at 408.

33. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (holding that a depositor in a bank assumes the risk that his information may be revealed to the government by sharing that information with a third-party).

34. *Miller*, 425 U.S. at 442-43.

35. *See, e.g.*, 12 U.S.C § 3405 (2012) (Financial Privacy Act).

36. *Miller*, 425 U.S. at 439.

37. *Id.*

38. *See id.* at 440 (holding that the depositor's financial records are not protected by the Fourth Amendment because the depositor can assert no ownership or control over financial records as they are the business records of the bank).

investigators subpoenaed financial transaction records, there was no Fourth Amendment violation because the accounts were the business records of the bank and "respondent could assert neither ownership nor possession."[39] Congress responded to this ruling with the passage of the Right to Financial Privacy Act of 1978,[40] which provides that no government authority may obtain a customer's financial records stored with a financial institution unless the government authority obtains, "a subpoena, a summons, a search warrant, or the customer's written consent, or unless the government submits a formal written request that complies with certain procedural requirements."[41]

Congress also attempted to increase privacy protection through the Stored Communications Act of 1986.[42] This Act requires the government to give "specific and articulable facts"[43] showing reasonable grounds to believe that the information is "relevant and material to an ongoing criminal investigation,"[44] when seeking a court order for third-party disclosure of non-content information.[45] "Non-content information"[46] has been defined as "information that facilitate[s] personal communications, rather than part of the content of those communications themselves,"[47] such as "mailing addresses, phone numbers, and IP addresses."[48]

Recently, the Supreme Court in *Carpenter v. United States* carved out an exception to the Stored Communications Act for a particular type of non-content information: cell site location information ("CSLI") from cell phone carriers.[49] CSLI is a time-stamped record that is generated every time a device such as a cell phone taps into a wireless

39. *Id.*

40. Duncan v. Belcher, 813 F.2d 1335, 1337 (4th Cir. 1987); 12 U.S.C § 3405 (2012).

41. *Duncan*, 813 F.2d at 1337.

42. 18 U.S.C. §§ 2701–2712 (2012).

43. *Id.*

44. *Id.* Note that this standard is still less than a showing of "probable cause" as is required for a warrant, but it is still an effort by Congress to increase privacy protection.

45. 18 U.S.C. § 2703(d) (2012).

46. The Stored Communications Act, *see* § 2703(c)(2) (enumerating some examples that fall into the non-content category).

47. United States v. Graham, 824 F.3d 421, 433 (4th Cir. 2016).

48. *Id.*

49. *See generally*, Carpenter v. United States, 138 S. Ct. 2206, 2206-22 (2018) (holding that CSLI is distinguishable from other types of non-content information and deserves Fourth Amendment protection).

network by connecting to a set of radio antennas called "cell sites."[50] Cell sites are found at the top of cell towers and on buildings, light posts, and flagpoles.[51] Generally, cell sites have directional antennas that are divided into sectors, with each sector covering a different geographic area.[52] These geographic areas have gotten increasingly smaller over time, allowing for more precise location information as cell phone usage increased and wireless carriers had to install more cell sites.[53] Not only is CSLI precise, but it is also constant; cell phones are continuously scanning for the best signal from the nearest cell site even when users are not actively making calls or sending texts.[54]

III. A NEW CARVE-OUT FOR CSLI

The *Carpenter* story begins in 2011 when "police officers arrested four men suspected of robbing a series of Radio Shack and (ironically enough) T-Mobile stores in Detroit."[55] One of the men confessed that the group had robbed nine different stores over the previous four months.[56] The suspect identified fifteen accomplices and revealed some of their cell phone numbers.[57] Then, FBI agents reviewed the suspect's call records to find other numbers he contacted around the time of the robberies.[58]

Based on the intelligence gained from the suspect, the prosecutors sought a court order under the Stored Communications Act to obtain Timothy Carpenter's cell phone records.[59] Federal magistrate judges ordered both MetroPCS and Sprint, Carpenter's wireless carriers, to disclose CSLI at call origination and termination of both incoming and outgoing calls during the four-month period of the robberies.[60] The first order to MetroPCS sought 152 days of CSLI, while the order to Sprint requested

50. *Carpenter*, 138 S. Ct. at 2211.
51. *Id.*
52. *Id.*
53. *Id.* at 2211-12.
54. *Id.* at 2211.
55. *Id.* at 2212.
56. *Id.*
57. *Id.*
58. *Id.*
59. *Id.*
60. *Id.*

seven days of CSLI, for a grand total of 12,898 location points.[61] The CSLI placed Carpenter—or at least, his phone—near four of the charged robberies.[62] Carpenter was convicted of all but one of the armed robberies and sentenced to over 100 years in prison.[63]

Upon review of the constitutionality of the CSLI obtained without a warrant, the Supreme Court held that CSLI deserves to be treated as an exception to the Stored Communications Act.[64] Due to the unique nature of CSLI, the mere fact that the information is held by a third-party does not bar a Fourth Amendment claim.[65] Individuals have a reasonable expectation to privacy in the whole of their physical movements,[66] as evidenced by prior case law.[67] Given that cell phones are so prominent in everyday life,[68] the court went so far as to call cell phones "almost a 'feature of human anatomy'"[69] and stated that the location records offer an intimate window into a person's life,[70] with "rapidly approaching GPS-level precision."[71] Due to the ubiquitous use of cell phones in everyday life, the increasing precision of CSLI, and the fact that location services are constantly running even without use of the phone, the court made a narrow ruling that this type of record stored with a third-party requires a warrant.[72]

Before forecasting the future, it is worthwhile to examine how the *Carpenter* decision affects the third-party doctrine and suppresses private information.[73] Currently, courts are admitting historical cell-site data if

---

61. *Id.*
62. *Id.* at 2213.
63. *Id.*
64. *Id.* at 2217.
65. *Id.*
66. *Id.*
67. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (analyzing society's reasonable expectation of privacy in the sum of an individual's movements); *see also* Riley v. California, 134 S. Ct. 2473, 2490 (2014) (holding that the data contained in defendant's cell phone deserves Fourth Amendment protection for several reasons, including the historic location data that can "reconstruct someone's specific movements down to the minute").
68. *Carpenter*, 138 S. Ct. at 2220.
69. *Id.* at 2218.
70. *Id.* at 2217-18.
71. *Id.* at 2219.
72. *Id.* at 2222.
73. *See id.* at 2220 (stating that when analyzing new innovations, it is important to tread carefully).

that data was collected before the June 22 *Carpenter* decision.[74] These courts admit this data through the exclusionary rule's good faith exception,[75] which states that "when investigators 'act with an objectively reasonable good-faith belief that their conduct is lawful,' then the exclusionary rule will not apply."[76] The Supreme Court has held that searches conducted in "reasonable reliance on subsequently invalidated statutes"[77] fall well within this good faith exception.[78] Therefore, a warrant will only be required for investigators who begin to seek CSLI after June 22, 2018.[79]

IV. BLOCKCHAIN: HOW IT WORKS, AN INSIDE LOOK AT BITCOIN PROTOCOLS, AND THE PROS AND CONS OF THE BLOCKCHAIN NETWORK

Although *Carpenter* is a narrow holding,[80] the case could have lasting impact on technological advances similar to CSLI.[81] Blockchain is one example of a similar technological advancement.[82] In its simplest form, blockchain is a shared network that lets members record a history of transactions on an immutable ledger.[83] The network establishes trust, accountability, and transparency through a system of granting permission to trusted users.[84] Permissioned users can manage, adjust, and restore entries on the ledger and all other nodes (members) confirm that the

74. Daniel R. Stoller, *Second Federal Appeals Court Allows Cell-Site Data as Evidence (1)*, PRIVACY L.WATCH (BNA) (August 28, 2018).

75. *See, e.g.,* United States v. Chavez, 894 F.3d 593, 608-09 (4th Cir. 2018) (denying the defendant Fourth Amendment protection for CSLI obtained by law enforcement officers in good faith).

76. *Id.* at 608 (citing Davis v. United States, 564 U.S. 229, 239 (2011)).

77. *Id.*

78. *Id.*

79. Stoller, *supra* note 74.

80. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

81. *See* Sandick, *supra* note 16 (suggesting that courts may extend privacy protections to other types of technological records that are similar to CSLI).

82. *See How do Bitcoin Transactions Work?*, COINDESK (Jan. 29, 2018), https://www.coindesk.com/information/how-do-bitcoin-transactions-work/ (describing the functionality of blockchain transactions).

83. Brittany Manchisi, *What is Blockchain Technology?*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (July 31, 2018), https://www.ibm.com/blogs/blockchain/2018/07/what-is-blockchain-technology/.

84. *Id.*

transaction is valid.[85] This agreement is called a "consensus,"[86] and relates back to the idea of transparency, since each node can see every transaction.[87] Once consensus is reached, the records are permanently stored on the ledger.[88] Consequently, the ledger provides more accountability because each entry can forever be tied back to the participants.[89] The immutability of the ledger instills trust: since blocks cannot be changed after they are created, members of the network can trust that the information on the ledger is authentic.[90]

While we know blockchain has many different applications,[91] we must draw the distinction between blockchain for Bitcoin and blockchain for business.[92] First, Bitcoin and blockchain are not synonymous terms for one another; their relationship is likely confused because they were released at the same time and Bitcoin was the first application of blockchain.[93] Bitcoin is a type of virtual currency, also known as a "cryptocurrency."[94] Bitcoin was developed to circumvent government regulations and other controls and to cut out the intermediary in most currency exchange platforms, providing for cheaper and more efficient ways to exchange money.[95] Bitcoin transactions are stored on distributed ledgers, using blockchain technology.[96]

Blockchain for business is slightly different from blockchain for Bitcoin, although the underlying technology is the same.[97] In an unregulated world of Bitcoin, blockchain is an open, public, and anonymous network with a distributed ledger full of Bitcoin transactions.[98] In contrast, blockchain business transactions involve assets other than

85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. *Id.*
90. *Id.*
91. BLOCKGEEKS, *supra* note 11.
92. Lucas, *supra* note 3.
93. Lucas, *supra* note 3.
94. Lucas, *supra* note 3.
95. *See, e.g. Bitcoin: Examining the Benefits and Risks for Small Business: Hearing Before the Comm. on Small Business*, 113th Cong., 4, (2014) (statement of Jerry Brito, Senior Research Fellow, Mercatus Center, George Mason University).
96. *Id.* at 22.
97. Lucas, *supra* note 3.
98. Lucas, *supra* note 3.

cryptocurrencies, such as real estate, food products, and securities.[99] Members in blockchain for business cannot be anonymous due to strict Know Your Customer ("KYC") and anti-money laundering ("AML") laws.[100] Lastly, blockchain for business relies on "selective endorsement"[101] instead of "mining."[102] Mining is a term that refers to the process where all the nodes have to reach a consensus before a transaction is recorded.[103] "Selective endorsement,"[104] by contrast, is where specific members are granted authority to verify the transaction.[105]

There are a few other terms and concepts that are helpful to fully understand the functionality of blockchain.[106] The following analysis focuses on these concepts in the context of Bitcoin, but there are many other cryptocurrencies that may follow different protocols.[107] These protocols may also vary in modified blockchain applications for business, but will provide us with a close look at how the original blockchain technology functions.[108]

First, Bitcoin transactions operate around public keys and their corresponding private keys.[109] A public key is made up of a string of thirty-four letters and numbers, referred to as a "Bitcoin address."[110] Contrary to the logical assumption, Bitcoin wallets do not hold any currency, but instead hold the user's public key, which keeps a record of all

99. Lucas, *supra* note 3.

100. Alexander Carmichael, *Insight: Blockchain Helps Banks Streamline Know Your Customer Processes*, WORLD SEC. L. REP. (BNA) (Aug. 15, 2018).

101. Lucas, *supra* note 3.

102. Lucas, *supra* note 3.

103. Lucas, *supra* note 3.

104. Lucas, *supra* note 3.

105. Lucas, *supra* note 3.

106. *See* Caitlin Long, *Supreme Court And Digital Privacy: Should Blockchain Companies Challenge The Bank Secrecy Act?*, FORBES (Jun. 28, 2018, 1:25 PM), https://www.forbes.com/sites/caitlinlong/2018/06/28/supreme-court-and-digital-privacy-should-blockchain-companies-challenge-the-bank-secrecy-act/#5f31a06162fc (projecting that other technologies that are similar to CSLI will likely want to litigate under the new ruling in *Carpenter*).

107. *See 10 Cryptocurrencies Other Than Bitcoin Which Are Changing The Crypto World*, COINSWITCH (13 July, 2018), https://coinswitch.co/news/10-cryptocurrencies-other-than-bitcoin-which-are-changing-the-crypto-world (detailing a list of other cryptocurrencies).

108. *See* Lucas, *supra* note 3 (explaining that Bitcoin was the first application of blockchain and that the blockchain technology was originally developed to meet the needs of that application).

109. *See How do Bitcoin Transactions Work?*, *supra* note 82 (explaining the functions of private keys and public keys in Bitcoin transactions).

110. *Id.*

of the user's transactions and therefore the user's balance.[111] The corresponding private key is much longer, made up of sixty-four letters and numbers.[112] While these keys are related, the Bitcoin system is encrypted such that there is no way for anyone to figure out the private key from the public key.[113] With that being said, it is crucial to keep the private key safe, because anyone with the private key can access the user's Bitcoin wallet.[114]

Another important concept in Bitcoin transactions is the "hash,"[115] or complex math function that "reduces any amount of text or data to a 64-character string."[116] Every time the blockchain system enters the same text or data into the hash function, it spits out the same response.[117] However, "if you change so much as a comma, you'll get a completely different 64-character string."[118] This helps the Bitcoin ledger flag any tampered transactions, making it virtually impossible to alter any after completion.[119]

Lastly, it is important to understand how the distributed ledger system works.[120] A distributed ledger is unlike traditional paper-based versions of accounting, because it is a network that is entirely held and updated by the participants (or nodes).[121] After someone uses Bitcoin, miners complete a series of complex math equations to verify the legitimacy of the transaction.[122] "Miners," refers to the computers that are spread out across the world and solve these complex equations.[123] This

111. *Id.*
112. *Id.*
113. *Id.*
114. *Id.*
115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. Curtis Miles, *Blockchain Security: What Keeps Your Transaction Data Safe?*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (Dec. 12, 2017) https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/.
120. *See* Nolan Bauerle, *What is a Distributed Ledger?*, COINDESK https://www.coindesk.com/information/what-is-a-distributed-ledger/ (last visited Feb. 9, 2019) (emphasizing the important role of distributed ledgers in blockchain transactions).
121. *Id.*
122. Lucas, *supra* note 3.
123. *Bitcoin Mining Explained*, INVESTOPEDIA.COM https://www.investopedia.com/terms/b/bitcoin-mining.asp (updated Dec. 19, 2018).

mining process creates a "proof of work," or a piece of data that shows the miners have reached a consensus.[124] Whenever a transaction is made, a "block"[125] transmits the relevant Bitcoin addresses, digital signatures, timestamps, amounts, and any other relevant information to all other participants in the network.[126] Each participant processes every transaction and holds a copy of the entire ledger for themselves.[127] In this way, the network is decentralized, lacking any one singular authority and providing more security.[128]

The functionality of the blockchain program and Bitcoin transactions has several pros and cons.[129] As SEC Chairman Clayton stated, at least one potential harm of cryptocurrencies is that "[their] features may facilitate illicit trading and financial transactions."[130] One real life example of the use of cryptocurrencies to facilitate illicit transactions can be found in the deep web and the dark web.[131] The "deep web" refers to the part of the internet that most users never see because it is not indexed in search engines, like Google.[132] The "dark web" refers to a small section of the deep web that can only be accessed with specific software or configurations.[133] One such section of the deep web took the form of a marketplace called SilkRoad,[134] which was created to facilitate "victimless crimes," such as the purchase of illegal drugs.[135] While the original SilkRoad has been permanently shut down,[136] the fear remains that blockchain and cryptocurrencies are the perfect platform for illegal activity.[137]

---

124. Lucas, *supra* note 3.

125. Bauerle, *supra* note 120.

126. Bauerle, *supra* note 120.

127. Bauerle, *supra* note 120.

128. Manchisi, *supra* note 83.

129. Clayton, *supra* note 6.

130. Clayton, *supra* note 6.

131. Andrew Norry, *The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin*, BLOCKONOMI (July 24, 2018), https://blockonomi.com/history-of-silk-road/.

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.*

137. *See* Frederick Coleman, *The Dark Side of Bitcoin: Illegal Activities, Fraud, and Bitcoin*, BLOCKONOMICS BLOG (Jun. 16, 2017), https://blog.blockonomics.co/the-dark-side-of-bitcoin-illegal-activities-fraud-and-bitcoin-360e83408a32 (demonstrating how criminals have used Bitcoin to conduct crimes and some people's fears that Bitcoin has done nothing but allow crime to grow).

However, there are numerous benefits of cryptocurrencies that the SEC Chairman also recognizes, like "(1) the ability to make transfers without an intermediary and without geographic limitation, (2) finality of settlement, (3) lower transaction costs compared to other forms of payment and (4) the ability to publicly verify transactions."[138] The benefits do not end there.[139] Cryptocurrency transactions help defend against fraud with their unique validation system.[140] In addition to the ability to publicly verify transactions on the ledger,[141] every transaction is validated through the recorded signatures of public keys and their corresponding private keys, which are impossible to discern from each individual public key.[142]

Further, the blockchain program supposedly guards against fraud.[143] The program plugs in the signature of the public key to confirm that Person A actually owns the money that Person A is transferring to Person B, and that Person A has not already sent the money to someone else.[144] The program can verify that the signature was made with the properly corresponding private keys, without even knowing what the private key is, resulting in heightened security while maintaining privacy.[145] Moreover, transactions are extremely difficult to alter once the transaction is validated and complete, because it would mean re-doing all the blocks that came after with a new hash, or code, further protecting transactions from fraud.[146]

Blockchain and cryptocurrencies are also useful in protecting against identity theft in financial transactions.[147] In comparison, credit

138. Clayton, *supra* note 6.

139. *See, e.g.*, Ameer Rosic, *5 Amazing Benefits of Cryptocurrency: A New Digital Future,* BLOCKGEEKS (2018), https://blockgeeks.com/5-benefits-cryptocurrency/ (describing numerous major benefits of cryptocurrencies including: fraud protection, identity theft protection, immediate settlement, access to everyone, and lower fees).

140. *See How do Bitcoin Transactions Work?*, *supra* note 82 (explaining how difficult it is to alter the ledger and how each person's identity and representations are validated through the system).

141. Bauerle, *supra* note 120.

142. *How do Bitcoin Transactions Work?*, *supra* note 82.

143. Rosic, *supra* note 139.

144. *How do Bitcoin Transactions Work?*, *supra* note 82.

145. *See How do Bitcoin Transactions Work?*, *supra* note 82 (discussing the relationship of public and private keys to functionality and security).

146. *How do Bitcoin Transactions Work?*, *supra* note 82.

147. Rosic, *supra* note 139.

cards are quite weak in this respect.[148] For example, when a consumer provides her credit card to a merchant, she gives the merchant access to her full line of credit, regardless of the size of transaction.[149] This access stems from the credit card's "pull" basis of operation, "where the store initiates the payment and pulls the designated amount from your account."[150] By contrast, cryptocurrency uses a much more secure "push" system, "that allows the cryptocurrency holder to send exactly what he or she wants to the merchant or recipient with no further information."[151]

Another way cryptocurrencies are beneficial to society is their low barrier to entry.[152] Roughly 2.2 billion people across the globe have access to the Internet or mobile phones, but do not have access to traditional money exchange systems.[153] In Kenya, for example, many people can access the internet but either have limited or no access to traditional bank accounts.[154] A solution to this problem came in the form of M-PESA, [155] a mobile phone-based money transfer and financing service that recently partnered with Bitwala, a blockchain service that allows Bitcoin transfers into M-PESA accounts.[156] One in three Kenyans now own a Bitcoin wallet as a result of this service.[157] Since M-PESA allows money to be sent directly from mobile phone to mobile phone, the barrier to entry for exchanging money through this currency is quite low.[158] A 2016 study by researchers from Georgetown and MIT shows that M-PESA's expansion has lifted nearly 200,000 Kenyan households above the poverty line.[159]

V. PRIVACY PROTECTION: WHERE THE LAW STANDS NOW AND WHERE

148. *See* Rosic, *supra* note 139 (explaining why cryptocurrency transactions are more secure than credit card transactions).

149. Rosic, *supra* note 139.

150. Rosic, *supra* note 139.

151. Rosic, *supra* note 139.

152. Rosic, *supra* note 139.

153. Rosic, *supra* note 139.

154. Rosic, *supra* note 139.

155. Rosic, *supra* note 139.

156. Luke Parker, *Bitwala announces fee-free Bitcoin to M-Pesa service*, BRAVE NEW COIN (Mar. 6, 2017), https://bravenewcoin.com/insights/bitwala-announces-fee-free-bitcoin-to-m-pesa-service.

157. Rosic, *supra* note 139.

158. Parker, *supra* note 156.

159. Parker, *supra* note 156.

IT COULD GO

United States government officials are facing difficulty in determining whether and how to regulate blockchain.[160] Meanwhile, state regulators have begun to welcome all sorts of applications for blockchain,[161] such as smart contracts,[162] real estate records,[163] and registration of corporate shares.[164] As blockchain becomes more prevalent,[165] regulation of blockchain could change[166] and *Carpenter* may need to be revisited to see if the same carve-out can be applied to information stored with blockchain.[167]

A. The Current Regulatory Scheme for Blockchain and its Effect on Blockchain's Functionality.

While blockchain itself has many applications, "in most cases, only one particular blockchain application captured the attention of lawmakers—blockchain in finance."[168] This regulatory attention has been primarily focused on initial coin offerings ("ICOs")[169] and anti-money laundering ("AML") efforts.[170] AML efforts are displayed in the regulation of everyday transactions in cryptocurrencies, as regulated by

160. *Blockchain Regulation*, *supra* note 12.

161. Divya Joshi, *How the Laws & Regulation Affecting Blockchain Technology can Impact its Adoption*, BUS. INSIDER (Oct. 20, 2017, 5:25 PM), https://www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global-2017-10.

162. ARIZ. REV. STAT. § 44-7061 (2018) (adding Article 5, "Blockchain Technology").

163. H.R. 120, 100th Gen. Assemb., Reg. Sess. (Ill. 2017).

164. 8 Del. C. § 224 (allowing records to be stored on "1 or more electronic networks or databases" and referring to a stock "ledger" rather than a stock "list").

165. Joshi, *supra* note 161.

166. Trevor I. Kiviat, *Beyond Bitcoin: Issues In Regulating Blockchain Transactions*, 65 DUKE L.J. 569 (2015).

167. *See* Sandick, *supra* note 16 (suggesting that courts may extend privacy protections to other types of technological records that are similar to CSLI).

168. *Blockchain Regulation*, *supra* note 12.

169. ICOs are fundraising attempts in which new cryptocurrency ventures sell coins to the public. They often resemble initial public offerings, where companies sell securities, but ICOs are not subject to securities regulations, making them prime avenues for fraudsters to defraud investors. *See* GREGORY G. JOHNSON, BRYAN CAVE LEIGHTON PAISNER LLP: VIRTUAL CURRENCIES, ICOS AND THE SEC (Jun. 1, 2018), https://www.bryancave.com/en/thought-leadership/virtual-currencies-icos-and-the-sec.html.

170. Kenneth A. Blanco, Director, FinCEN, Prepared Remarks at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block.

FinCEN.[171] FinCEN's leadership focuses on "exchangers, administrators, and other persons involved in money transmission denominated in convertible virtual currency."[172] In 2011, FinCEN issued a final rule indicating that "money transmission"[173] covers the acceptance and substitution for currency, such as virtual currency.[174] These money transmitters are responsible for complying with AML and countering the financing of terrorism ("CFT") requirements of the Bank Secrecy Act ("BSA").[175] The three main requirements include: (1) registering with FinCEN; (2) implementing an AML program to prevent money laundering and terrorist finance; and (3) maintaining recordkeeping and reporting requirements.[176]

The enforcement of these regulations dramatically changes the way blockchain functions.[177] AML and CFT compliance requirements impact the anonymity that Bitcoin used to thrive on, because network users must be known in order to make the requisite filings.[178] Participants in this setting "require the polar opposite of anonymity: privacy."[179] Participants need to see who they are dealing with directly, but do not need to see every transaction that has ever occurred.[180] This can be accomplished by setting up a permissioned network that places restrictions on who is allowed to participate in certain transactions.[181] Only the users participating in a particular transaction will have access to that particular block on the chain.[182] Access can be controlled by a regulatory authority, a consortium, or existing participants.[183] One example of a private blockchain network is the Linux Foundation's Hyperledger Fabric, where

171. *Id.*
172. *Id.*
173. *Id.*
174. *Id.*
175. 31 U.S.C. §§ 5311-5330 (2012); Blanco, *supra* note 170.
176. Blanco, *supra* note 170.
177. Lucas, *supra* note 3.
178. Lucas, *supra* note 3.
179. Lucas, *supra* note 3.
180. Lucas, *supra* note 3.
181. Praveen Jayachandran, *The difference between public and private blockchain*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (May 31, 2017), https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/.
182. *Id.*
183. *Id.*

participants are known but data is only shared with specific individuals through a series of permissions.[184]

B. The Future of Privacy Law and Blockchain: As Blockchain Becomes More Prevalent, Can Fourth Amendment Protection, Under Carpenter v. United States, Be Applied to Information Stored with Blockchain?

Before analyzing the future of privacy law in relation to blockchain, an important distinction needs to be made between the concepts of privacy and secrecy.[185] In general, secrecy is bad and privacy is good.[186] Secrecy means, "withholding information, even from people who have a legitimate right to access it."[187] Privacy means control of the sharing of information that one rightfully owns.[188] Privacy can be maintained within a public blockchain ledger.[189] Data in that ledger can be encrypted, which makes it only accessible to those with the specific encryption keys for the transaction.[190] Through this process, blockchain is able to remove secrecy while maintaining privacy.[191] Anyone can verify the transaction and ensure the data exists, but only the participants are allowed to access the data itself.[192]

In terms of legal protection, the Right to Financial Privacy Act likely does not afford any privacy protection to blockchain or Bitcoin.[193] The Act instills a warrant requirement for the recovery of bank records held by a financial institution.[194] A financial institution, in turn, is defined

184. *See Hyperledger: Blockchain Collaboration Changing the Business World*, IBM BLOCKCHAIN, https://www.ibm.com/blockchain/hyperledger?cm_mmc=OSocial_Blog-Blockchain+and+Watson+Financial+Services_Blockchain-_-WW_WW-_-The+difference+between+public+and+private+blockchain+In+Text+Hyperledger+Webpage&cm_mmca1=000026VG&cm_mmca2=10005805& (advertising IBM's private blockchain for business purposes and how it works).

185. MAD NETWORK, *supra* note 9.

186. MAD NETWORK, *supra* note 9.

187. MAD NETWORK, *supra* note 9.

188. MAD NETWORK, *supra* note 9.

189. MAD NETWORK, *supra* note 9.

190. MAD NETWORK, *supra* note 9.

191. MAD NETWORK, *supra* note 9.

192. MAD NETWORK, *supra* note 9.

193. *See* 12 U.S.C. § 3401(1) (2012) (defining "financial institution," for the purposes of this Act).

194. § 3406(a) (2012).

as "any office of a bank, savings bank, card issuer" or other traditional banking entity further described in the statute.[195] Bitcoin likely does not fit into any of these categories because it is a system of exchanging currency that circumvents the intermediary.[196] Furthermore, the Act is limited in scope to financial institutions within the United States and its territories.[197] Bitcoin transactions are conducted over the internet across users in varying countries,[198] so it would be difficult to say whether cross-border Bitcoin transactions fall within the location requirement for the Act to apply unless the particular application of blockchain had a more central authority.

However, if blockchain ledgers can fall under the definition of an electronic communication service, the Stored Communications Act likely applies.[199] The Stored Communications Act protects against intentional access of information without authorization from a facility through which an electronic communication service is provided.[200] Recall that the protection extended to non-content information under the Act is much less than the protection afforded in *Carpenter*.[201] Under the Act, law enforcement must only show "specific and articulable facts" to demonstrate reasonable grounds for believing the information is "relevant and material to an ongoing criminal investigation."[202] *Carpenter* raised this standard of proof to a showing of probable cause only for instances where law enforcement seeks to obtain CSLI.[203] Until further litigation, all other forms of electronic communication services remain under the lower

195. § 3401(1) (2012).

196. *See* Lucas, *supra* note 3 (explaining how blockchain first came in to existence as a solution to the desire to circumvent government controls through anonymity, security, and cutting out the intermediary).

197. Lucas, *supra* note 3

198. See Clayton, *supra* note 6 (stating that cryptocurrency and ICO markets are "local, national and international and include an ever-broadening range of products and participants.").

199. *See* 18 U.S.C. § 2701(a)(1) (stating that the Stored Communications Act applies to electronic communication services).

200. *Id.*

201. § 2703(d) (2012).

202. §§ 2701-2712 (2012).

203. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

standard of proof.[204] Furthermore, the Act does not extend any protection for information that is readily available to the public.[205] However, a United States district court recently held that even Facebook posts can be considered private and not readily available to the public.[206] The court held that, "the statute's purpose is to protect information that the communicator took steps to keep private."[207] Blockchain likely meets this test as blockchain users by definition take steps to keep their information private.[208] Therefore, if blockchain falls under the purview of the Stored Communications Act, *substantive* information stored with blockchain may be protected, while *non-content* information stored with blockchain is still subject to the lower standard of proof.[209] Law enforcement can therefore obtain this non-content information without a warrant.[210]

This raises the question of whether the *Carpenter* carve-out of the Stored Communications Act for CSLI can also be applied to blockchain. This question may depend on whether blockchain is as prevalent in society as cell phones.[211] While that currently is not yet the case, it may be worthwhile to examine what the future may bring. After all, mobile phones only first started appearing in the average consumer's hands between 1990 and 1995.[212] Now, they are almost a "feature of human

204. Sandick, *supra* note 16.

205. 18 U.S.C. § 2511(2)(g)(i) (2012).

206. Ehling v. Monmouth-Ocean Hosp. Service Corp., 961 F.Supp.2d 659, 668 (D.N.J. 2013).

207. *Id.*

208. *See* MAD NETWORK, *supra* note 9 (explaining how the data on public ledgers can remain private through encryption and permission keys).

209. The Stored Communications Act at 18 U.S.C. § 2703(c)(2) provides a list of examples of non-content information that can be obtained without a warrant. That list includes names, addresses, length of service, types of service utilized, "telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address," and the source of payment for such a service, including bank account information and card numbers.

210. § 2703(c)(1)(E).

211. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (discussing that the prevalence of cell phones has led to data that is "compiled every day, every moment, over several years.").

212. Richard Goodwin, *The History of Mobile Phones From 1973 To 2008: The Handsets That Made It ALL Happen*, KNOW YOUR MOBILE (Mar. 6, 2017), https://www.knowyourmobile.com/nokia/nokia-3310/19848/history-mobile-phones-1973-2008-handsets-made-it-all-happen.

anatomy."[213] At the rate technology develops today, a similar prevalence in consumer blockchain usage may be on the horizon.[214]

Upon further analysis, the underpinning technologies behind blockchain and CSLI are similar because (1) users of each have reasonable expectations of privacy[215] to the information collected, and (2) access to the information contained in any ledger block, like CSLI,[216] would be extremely intrusive.[217] Moreover, blockchain ledgers constantly make connections between each user's individual transaction on the ledger without the direct consent of the user.[218] This sharing of information becomes less voluntary as blockchain becomes more ubiquitous.[219]

Like cell phone users, blockchain users have a reasonable expectation to privacy in the information collected—their identities, who they transact with, their private keys, the time of the transaction, their IP addresses, and other information—while making transactions.[220] A long line of Supreme Court cases dedicated to defining reasonable expectations suggests that not only must the individual feel an expectation of privacy, but that expectation must be reasonable as demonstrated by societal recognition.[221] There is evidence that society recognizes a higher standard of privacy for blockchain ledgers: the platform itself was created to provide more secure and anonymous transacting,[222] proliferating

213. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)).

214. *See*, *e.g.*, Long, *supra* note 106 (projecting that blockchain may be one industry to soon follow the CSLI carve-out).

215. *See* MAD NETWORK, *supra* note 9 (explaining how even public ledgers have some privacy expectations built in to the way the network functions).

216. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that CSLI is so intrusive as to reveal the "privacies of life.").

217. *See, e.g.*, *How do Bitcoin Transactions Work?*, *supra* note 82 (explaining how transactions are recorded in the ledger and the privacy expectations of the user in protecting anonymity).

218. *See How do Bitcoin Transactions Work?*, *supra* note 82 (describing how hash codes instantly and automatically connect one transaction to another in the distributed ledger system).

219. *See Carpenter*, 138 S. Ct. at 2220 (2018) (holding that cell phone users do not voluntarily agree to the collection of CSLI because utilization of cell phones is so necessary to participation in modern society, and collection of CSLI is a mandatory condition of that utilization).

220. *See How do Bitcoin Transactions Work?*, *supra*, note 82 (describing the inherent privacy benefits of the blockchain system that users can take advantage of).

221. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

222. Bernard, *supra* note 4.

among users in the deep and dark webs,[223] and allowing for a system of anonymity.[224] Moreover, users have begun taking further steps to protect their privacy on the platform by conducting transactions from multiple wallets.[225] The expectation of privacy is likely stronger in blockchain for business, where networks and their ledgers are private and users must have permission to view a certain transaction and the transaction's participants.[226] However, as case law seems to be unclear on how to judge societal recognition of privacy, this may be a question for a fact-finder.[227] Moreover, this decision may be subject to whether society includes only users, who are familiar with the blockchain platform, or society at large, who may be unfamiliar with how the privacy aspects of blockchain work.[228]

Some may argue that there is no reasonable expectation to privacy in blockchain for cryptocurrencies because the transactions are recorded on a public ledger that anyone can access.[229] However, as *Carpenter* illustrated, a person does not lose their expectation of privacy under the Fourth Amendment by merely "venturing into the public."[230] For example, in *Katz*, the defendant did not lose his right to privacy in his telephone conversations merely because he made the call from a public phone booth.[231] As Justice Roberts reiterated in his majority opinion in *Carpenter*, "what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[232] It follows that even though transactions are recorded on a public ledger, the ledger data

223. Norry, *supra* note 134.

224. *See How do Bitcoin Transactions Work?*, *supra* note 82 (explaining how public and private keys work to protect anonymity of the user).

225. Lielacher, *supra* note 1.

226. Jayachandran, *supra* note 181.

227. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (stating the expectation of privacy must be one that is reasonable and that society is prepared to recognize, but giving not instruction on how to determine what society is willing to recognize).

228. *See id.* (stating the expectation of privacy must be one that is reasonable and that society is prepared to recognize, but failing to define "society" in any particular way).

229. *See* Bauerle, *supra* note 120 (explaining how the distributed ledger system is viewable by the public).

230. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

231. *Katz*, 389 U.S. at 253-53.

232. *Carpenter*, 138 S. Ct. at 2217 (quoting *Katz*, 389 U.S. at 351-42 (internal alteration omitted)).

can still be constitutionally protected so long as the users seek to preserve this information as private.[233]

Blockchain ledgers are also like CSLI in that each block in the chain provides "an intimate window into a person's life, revealing . . . familial, political, professional, religious, and sexual associations."[234] Blockchain ledgers for cryptocurrency, like CSLI, can reveal much about a person's life, such as the amount, date, and time of transactions as well as who they are contracting with, selling to, and buying from.[235] For example, Coinbase, a cryptocurrency exchange platform headquartered in San Francisco, warns in its privacy policy that the platform collects the consumer's "name, date of birth, social security number, driver number ID, personal ID, address, phone, email, [and] full bank account details" used in creating an account.[236] Coinbase collects additional information as it carries out the service.[237]

Blockchain for business presents even worse consequences of exposure.[238] In healthcare industries, blockchain can be used to hold sensitive patient records.[239] In the Internet of Things subpoena of the ledger could reveal daily activities and movements based on synched internet calendars, GPS systems, cell phones, and much more.[240] The risk of the exposure of just one block is magnified as it expands to other users, because each block contains a hash that connects to another block, and that block connects to another, and so forth until all the blocks in the chain are revealed.[241] This presents a further issue to consider: whether the subpoena of one block has the potential to reveal personal information

233. See *Katz*, 389 U.S. at 352 (holding that private telephone conversations do not lose their privacy protection merely because they are made from public phone booths).

234. *Carpenter*, 138 S. Ct. at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

235. *See* Bauerle, *supra* note 120 (describing some of the information stored in a block).

236. *Coinbase Privacy Policy*, COINBASE, https://www.coinbase.com/legal/privacy (last updated May 16, 2018).

237. *Id.*

238. *See, e.g.* Udit Sharma, *Blockchain in healthcare: Patient benefits and more*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (Oct. 30, 2017), https://www.ibm.com/blogs/blockchain/2017/10/blockchain-in-healthcare-patient-benefits-and-more/ (describing how blockchain can be used to keep sensitive patient records).

239. *Id.*

240. *Blockchain Applications Transforming Society*, *supra* note 11.

241. *See How do Bitcoin Transactions Work?*, *supra* note 82 (explaining how hashes work to automatically connect blocks to one another).

about others, or if it can be limited to just one suspect in an investigation.[242]

Moreover, blockchain ledgers are similar to CSLI because hash connections are similar to the constant connections phones make to cell sites.[243] Cell phones constantly search for signals, even when the phone is not in use by its owner.[244] Likewise, blockchain ledgers connect transactions to other transactions both before and long after the user makes his own transaction.[245] The user does not choose which blocks his block gets attached to, and is thereby forced into exposure should any of those other blocks get subpoenaed.[246] Some may argue that this exposure is voluntary since the user likely knows how the blockchain ledger works and assumes the risk.[247] In fact, users of exchange platforms like Coinbase have to agree to a privacy policy which lays out how and with whom their confidential information may be shared.[248] However, a similar argument was raised in *Carpenter*, and the Supreme Court held that the sharing of information is not truly voluntary where doing so is mandatory to participate in modern society.[249] Again, for blockchain to have a winning argument here, it would have to reach the same level of prevalence in modern society as cell phones.[250]

Blockchain may one day be so ubiquitous as to become "indispensable to participation in modern society,"[251] much like cell phones are today.[252] While blockchain in the United States is not there yet, there is ample evidence that countries all over the globe are actively seeking to integrate blockchain and cryptocurrencies into modern society.[253]

---

242. *How do Bitcoin Transactions Work?*, *supra* note 82.

243. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

244. *Id.* at 2211.

245. *See How do Bitcoin Transactions Work?*, *supra* note 82 (describing how hash codes instantly and automatically connect one transaction to another in the distributed ledger system).

246. *How do Bitcoin Transactions Work?*, *supra* note 82.

247. *See Carpenter*, 138 S. Ct. at 2220 (making a similar argument against CSLI).

248. *Coinbase Privacy Policy*, *supra* note 236.

249. *Carpenter*, 138 S. Ct. at 2220.

250. *Id.*

251. *Id.* at 2210, 2220 (citing Riley v. California, 134 S. Ct. 2206, 2484 (2014)).

252. *Id.*

253. *Blockchain Regulation, supra* note 12; *see also* Mike Orcutt, *Governments Are Testing Their Own Cryptocurrencies*, MIT TECH. REV. (Sept. 25, 2017), https://www.technologyreview.com/s/608910/governments-are-testing-their-own-cryptocurrencies/ (describing blockchain regulations in other countries).

Bitwala[254] allows consumers to instantly exchange cryptocurrencies into Euro, spend currencies in stores and online, and withdraw funds from any ATM worldwide.[255] Many major companies that sell everyday goods and services, such as Subway, PayPal, Overstock, and Expedia, have begun accepting cryptocurrencies.[256] There are currently over 3,700 Bitcoin ATMs worldwide, and an average of almost five new Bitcoin ATMs are installed every day.[257] Even North Carolina attorneys are starting to accept payment via cryptocurrency.[258] Cryptocurrencies and blockchain are quickly being integrated into modern society and could one day become just as ubiquitous as cell phones, therefore warranting greater privacy protection.[259]

VI. CONCLUSION

The United States is struggling to regulate blockchain because the technology is new and unique.[260] Other countries, however, are racing to integrate blockchain and cryptocurrencies into their societies and laws.[261] Therefore, it is in the United States' best interest to act quickly so as not to get left behind.[262] In the coming years, the United States may be faced with the question of whether to extend privacy protections to the information stored on blockchain ledgers.[263]

---

254. Bitwala is a company that combines traditional banking features with cryptocurrency banking features, and recently released a Bitcoin debit card through Mastercard. *Blockchain Banking*, BITWALA (2018), https://www.bitwala.com/.

255. *Id.*

256. *7 Major Companies That Accept Cryptocurrency*, NASDAQ (Jan. 31, 2018), https://www.nasdaq.com/article/7-major-companies-that-accept-cryptocurrency-cm913745.

257. *Bitcoin ATM Industry Statistics / Charts*, COIN ATM RADAR (2018), https://coinatmradar.com/charts/#growth.

258. James M. McCauley et al., *Is it Ethical for Lawyer to Accept Bitcoins and Other Cryptocurrencies?*, N.C. ST. BAR (Sept. 3, 2018), https://www.ncbar.gov/for-lawyers/ethics/ethics-articles/is-it-ethical-for-lawyers-to-accept-bitcoins-and-other-cryptocurrencies/.

259. *See, e.g.*, *7 Major Companies That Accept Cryptocurrency*, *supra* note 257 (demonstrating how many everyday companies are beginning to accept cryptocurrencies as a form of payment).

260. *See Blockchain Regulation*, *supra* note 12 (stating that U.S. government officials lack economists with the proper blockchain expertise to make regulations).

261. *See Blockchain Regulation*, *supra* note 12 (describing blockchain regulations in other countries).

262. *See Blockchain Regulation*, *supra* note 12 (comparing blockchain regulations in other countries to the lack thereof in the U.S.).

263. *See* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) (holding that CSLI is an exception to the non-content information covered by the Stored Communications Act).

Carpenter may have opened the door for warrant requirements to be applied to blockchain and cryptocurrencies once they become more prevalent in modern society.[264] Once this occurs, legislators could start by updating the Stored Communications Act to explicitly exclude particular types of digital information, like CSLI and blockchain ledgers.[265] Another option would be to update the Financial Privacy Act to include blockchain and cryptocurrency platforms in the definition of financial institution.[266] Alternatively, courts could decide whether society recognizes a reasonable expectation to privacy in blockchain transactions.[267]

Legislators and judges will also have to grapple with various issues in drafting a warrant requirement for blockchain technologies.[268] Who or what exactly would the warrant be for?[269] Would the warrant be for an individual member's server or would it be broader to include an entire cryptocurrency exchange's ledger?[270] The answers to these questions may be illuminated over the next few years as we continue to learn about the functionality of different blockchain networks. Another issue is whether there needs to be different legal standards for different applications of blockchain.[271] As Trevor I. Kiviat stated in the Duke Law Journal, "[b]lockchain technology is adaptable and policymakers must view it as such."[272] Whatever laws go into effect will need to be carefully drafted or opined such as not to chill other blockchain applications.[273]

---

264. Long, *supra* note 106 (projecting that blockchain may be one industry soon to follow the CSLI carve-out).

265. *See supra* Part V.B (discussing blockchain's propensity to fit into the same carve-out as CSLI under the Stored Communications Act).

266. The Financial Privacy Act only applies to financial institutions as defined in the statute. 12 U.S.C. § 3401(1) (2012).

267. *See* Long, *supra* note 106 (quoting the ACLU attorney who argued *Carpenter*, in that the case "opens the door to safeguarding other sensitive digital information in many future cases. . .").

268. *See* Jay M. Zitter, *Error, in Either Search Warrant or Application for Warrant, as to Address of Place to be Searched as Rendering Warrant Invalid*, 103 A.L.R.5th 463, § 2[a] (2002) (enumerating the many issues law enforcement faces when obtaining a warrant).

269. *Id.* ("One of the specific commands of the Fourth Amendment to the United States Constitution is that no warrants shall be issued except those 'particularly describing the place to be searched.'")

270. *See* 18 U.S.C. § 2074 (2012) (applying only to entities that constitute "providers" of electronic communications services).

271. Trevor I. Kiviat, *Beyond Bitcoin: Issues In Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 607 (2015).

272. *Id.*

273. *Id.*

As the Supreme Court explained in *Carpenter*, we must tread carefully so as not to "embarrass the future"[274] by the hastiness of today, since technology can change in a heartbeat.[275] However, it is equally important to vigilantly monitor the trends in technology and the role blockchain has in society.[276] The dynamic duo, blockchain and Bitcoin, could easily one day become a basic "feature of human anatomy,"[277] or they could disappear as fast as they came, in the same fantasy-esque and mysterious manner as their anonymous creator.[278] Only time will tell.

ASHLEY N. LONGMAN[*]

274. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
275. *Id.*
276. Clayton, *supra* note 6.
277. *Carpenter*, 138 S. Ct. at 2218.
278. Bernard, *supra* note 4.

[*]I am particularly grateful to Professor Lissa L. Broome, Joanne Wu, Peter J. Cline, and the rest of the North Carolina Banking Institute editors and staff for their thoughtful comments and review during the editing process. I would also like to thank my family and friends for their support and encouragement throughout my law school career.