Building Blocks of Privacy: Why the Third-Party Doctrine Should Not Be Applied to Blockchain Transactions

Veronica Lark*

TABLE OF CONTENTS

[*] J.D., May 2022, The George Washington University Law School; B.A., English, May 2016, Lourdes University. I would like to thank Professor Ethan Lucarelli and Olivia Creser for their mentorship in the drafting this Note. Thank you as well to Professor Daniel Solove for his feedback on the privacy issues raised by my topic, and to Professor Douglas Pepe for his guidance concerning the technical aspects of this paper.

I. INTRODUCTION

In early 2018, twenty-three million users logged onto Coinbase, presumably to confirm how much Bitcoin had spiked in price or maybe to swap their Ethereum for Litecoin.[1] For months leading up to this, people were swarming to cryptocurrency exchanges like Coinbase to see "blockchain" in action. Many were told—by friends, acquaintances, their boss—a brief elevator pitch about cryptocurrency along the lines of: "cryptocurrency is the cash of the future!" or "blockchain works without any third party, so that means your finances are more secure, since no one can tell who you are based on the digits that get stamped into the blockchain." To the millions who signed up for a Coinbase account, cryptocurrency may have represented a libertarian solution to the encroachment of large financial institutions. To others, it was an opportunity to engage in criminal behavior, thinking that the blockchain could conceal it.

In the context of recent court decisions in which defendants claimed privacy rights for data records stored on the blockchain, consumers may be surprised to learn that cryptocurrency exchanges like Coinbase are not legally viewed any differently than other financial institutions and intermediaries.[2] When individuals transact with third-party entities, such as using a bank to wire money, courts have held that individuals lose any privacy interest in the data they have shared because (1) it was shared voluntarily, and sharing voluntarily means that the individual assumes the risk of the information being shared with the government, and (2) the individual does not own the business record.[3] This legal concept is known as the third-party doctrine. The result is that third parties like banks do not need to be presented with a search warrant before they turn over client records.[4] This legal reality extends into digital space, applying to those types of transactions conducted via credit card on third-party applications like Apple Pay and Venmo.[5]

Additionally, this legal reality implicates blockchain transactions.[6] However, there is a critical distinction between a blockchain and a third-party cryptocurrency exchange like Coinbase. A blockchain has no third-party intermediary—it is a digital ledger—in contrast with a cryptocurrency

[1] *See Global Number of Verified Coinbase Users from 1st Quarter of 2018 to 4th Quarter of 2020*, STATISTA (Mar. 2021), https://www.statista.com/statistics/803531/number-of-coinbase-users/ [https://perma.cc/9ETB-JE8L].

[2] *See* Zietzke v. United States, No. 19-cv-03761, 2020 WL 264394, at *13 (N.D. Cal. Jan. 17, 2020); United States v. Gratkowski, 964 F.3d 307, 312 (5th Cir. 2020).

[3] *See* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[4] *See Smith*, 442 U.S. at 745-46.

[5] *See generally* Dina Moussa, *Protecting Payment Privacy: Reconciling Financial Technology and The Fourth Amendment*, 1 GEO. L. TECHNOLOGY REV. 342, 344-45 (2017).

[6] *See generally Zietzke*, 2020 WL 264394 at *13; *Gratkowski*, 964 F.3d at 312-13.

exchange which serves essentially as a cryptocurrency brokerage.[7] Even though the blockchain and exchange are two distinct entities, law enforcement has successfully subpoenaed the Coinbase exchange with knowledge of recipient addresses: using this information to track down the accounts that sent cryptocurrency.[8] Cryptocurrency exchanges possess personal identification information for account holders, but this information does not carry over to a blockchain transaction;[9] at this point, this distinction does not prevent law enforcement from subpoenaing cryptocurrency exchanges when searching for account holders' information that may be connected to a given blockchain transaction even when the search is speculative and not based on probable cause.[10] In *U.S. v. Carpenter*, the Supreme Court recognized a privacy interest for a specific emerging technology, cell site location information (CSLI).[11] As another form of an emerging technology, blockchain should fit within the framework used by the Supreme Court in *Carpenter*. Even though the blockchain reveals cryptocurrency transactions to the public, the technology that allows for this revelation of data does not reveal the personally identifiable information shared with the cryptocurrency exchange: there is a distinction between the exchange's business records and the blockchain transaction.[12] The blockchain ledger is not a third-party intermediary, and, thus, any request issued to a cryptocurrency exchange to acquire accountholder information based on separate decentralized ledger transactions should require that law enforcement acquire a search warrant. Once law enforcement has identified a unique public address engaging in fraudulent or illegal transactions recorded in the blockchain ledger, this should require law enforcement to present a search warrant to a cryptocurrency exchange to obtain the records, since law enforcement does not yet have the requisite reasonable suspicion of a particular accountholder,

[7] *See What's the Difference Between Coinbase.com and Coinbase Wallet?*, COINBASE, https://help.coinbase.com/en/wallet/getting-started/what-s-the-difference-between-coinbase-com-and-wallet (last visited Oct. 20, 2021); *see also* Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV., Jan.-Feb. 2017, https://hbr.org/2017/01/the-truth-about-blockchain [https://perma.cc/XV6G-7N66].

[8] *See Gratkowski*, 964 F.3d at 309.

[9] *See Data Privacy at Coinbase*, COINBASE, https://help.coinbase.com/en/coinbase/privacy-and-security/data-privacy/what-is-the-gdpr (last visited Oct. 20, 2021); *see also What is a Transaction Hash/Hash ID?*, COINBASE, https://help.coinbase.com/en/coinbase/getting-started/crypto-education/what-is-a-transaction-hash-hash-id (last visited Oct. 20, 2021).

[10] *See Gratkowski*, 964 F.3d at 309.

[11] *E.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[12] *See Public and Private Keys*, BLOCKCHAIN.COM SUPPORT, (Dec. 29, 2021, 6:21 AM), https://support.blockchain.com/hc/en-us/articles/360000951966-Public-and-private-keys (an individual's address is "a shorter, representative form of the public key" which is visible in a blockchain transaction and can be "derived using a known algorithm").

and they will not know the accountholder's identity until the exchange turns over its relevant records.[13]

Part II lays out the factual background necessary to understand blockchain, cryptocurrency, and cryptocurrency exchanges. Part III assesses the origins of privacy law, the evolution of the third-party doctrine, and the application of the third-party doctrine in blockchain cases. Part IV proposes and analyzes why the distinction between blockchains and cryptocurrency exchanges is critical in third-party doctrine analysis. Part IV, Section A presents the basis for finding a privacy right in blockchain data in the context of *Carpenter*. Part IV, Section B looks at the distinction made between publicly revealed information and private information, and positions blockchain and cryptocurrency exchanges within this framework. Part IV, Section C proposes that law enforcement should be required to obtain a search warrant when seeking account information possessed by a cryptocurrency exchange. Part V presents potential solutions using both the court system and Congress, and also asserts why the blockchain/cryptocurrency exchange distinction does not overextend *Carpenter* and responds to potential issues concerning actors who will try to evade criminal liability based on the blockchain/cryptocurrency exchange distinction. Part VI concludes this analysis.

II. BLOCKCHAIN, CRYPTOCURRENCY, AND CRYPTOCURRENCY EXCHANGES

This section provides a basis for understanding the components of a blockchain such as the decentralization of the blockchain, the nature of the ledger, and how cryptocurrency fits into this system. This section also explains the anonymity and permanence of cryptocurrency transactions and how a public transaction effectuates these qualities. This section also explains the technical qualities of a cryptocurrency exchange and how an exchange exerts control over users.

A. A Blockchain Is a Decentralized Public Ledger Allowing for the Execution and Storage of Cryptocurrency Transactions

Blockchain is a decentralized network comprised of a system of computer node participants that record transactions on a shared, immutable

[13] *See id.*; *see also* Tyler G. Newby & Ana Razmazma, *An Untraceable Currency? Bitcoin Privacy Concerns*, FINTECH WKLY., (Apr. 7, 2018), https://fintechweekly.com/magazine/articles/an-untraceable-currency-bitcoin-privacy-concerns [https://perma.cc/TMX4-BQ6Z]; *Reasonable Suspicion*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/reasonable_suspicion ("Reasonable suspicion is used in determining the legality of a police officer's decision to perform a search." Law enforcement does not have reasonable suspicion that a given accountholder is connected to a crime; they just have information about the digits identifying a specific account) [https://perma.cc/Q4T8-XMH8].

ledger.[14] Blockchain technology does not require a centralized third party, like a bank, to complete and store transactions; all participants share ownership of records so that no one user has full control.[15] The blockchain ledger is distributed because multiple computer nodes have authority to update the record on the ledger; there is no centralized party in control.[16] The nodes are essentially a network of computers that compete to complete mathematical equations under a given consensus protocol, and the computer that does this this computation correctly, and the most quickly, posts the entry into the ledger, thus adding a new block to the chain.[17] The "blocks" added to the ledger per transaction are immutable, in that with time it becomes computationally and economically impractical to reverse transactions, unlike the ease with which a transaction can be reversed or refunded in the traditional sense of being able to cancel a payment on a credit card.[18] A more accessible analogy in understanding the blockchain would be to imagine a web of computers that all have access to the same Google spreadsheet, and whenever a transaction occurs, it is entered into the spreadsheet after each participant races to complete a computation that confirms the validity of the transaction on the shared spreadsheet.[19] The spreadsheet entry cannot be edited and it is visible to everyone with access.[20]

Key for the purposes of this Note's analysis is whether a blockchain is public, private, hybrid, or permissioned, which will determine how much information parties implicitly share with others as a result of a transaction.[21] These distinctions essentially determine how transactions are fulfilled by a consensus to post transactions to the ledger.[22] Consensus varies in these circumstances and essentially involves mathematical computing to allow for digital entry of a transaction.[23] These types of chains allow different levels of participation in consensus and access to the ledger, but consensus does not equal ownership.[24] A public blockchain allows any participating computer to help reach consensus of a transaction; private blockchains allow only a portion of the participating computers to be part of the consensus; a hybrid blockchain allows the same level of participation as a public blockchain, but there are designated nodes that are the only ones to input a block; a permissioned blockchain is even more restrictive than a private blockchain,

[14] *See* Ashley N. Longman, *The Future of Blockchain: As Technology Spreads, it May Warrant More Privacy Protection for Information Stored with Blockchain*, 23 N.C. BANKING INST. 111, 118-19 (2019).

[15] *See* Iansiti & Lakhani, *supra* note 7.

[16] *See* Brittany Manchisi, *What is Blockchain Technology?*, IBM: SUPPLY CHAIN & BLOCKCHAIN BLOG (July 31, 2018), https://www.ibm.com/blogs/blockchain/2018/07/what-is-blockchain-technology/ [https://perma.cc/C65D-2B8V].

[17] *See* Suyash Gupta & Mohammad Sadoghi, *Blockchain Transaction Processing*, *in* ENCYCLOPEDIA OF BIG DATA TECHNOLOGIES 2-3 (2018).

[18] *See* Zibin Zheng et al., *Blockchain Challenges and Opportunities: A Survey*, 14 INT'L J. WEB & GRID SERVS. 352, 357 (2018); *see also* Longman, *supra* note 14, at 119.

[19] *See* Zheng, *supra* note 18, at 354-55.

[20] *See id.*

[21] *See* Gupta & Sadoghi, *supra* note 17, at 3.

[22] *See id.*

[23] *See id.*

[24] *See id.* at 3-4.

and allows only a certain select group of computer nodes to participate in the consensus process.[25] Each node participant has its own copy of the ledger, which is constantly updated with new transaction entries; this distribution of the ledger makes it difficult for any one party to alter past data entries.[26] These different levels of permission and access are also wholly separate from the discussion of the cryptocurrency exchange: where transactions are buys and sells that are fulfilled by the cryptocurrency exchange and maintained in accounts owned by the exchange, and this transaction history and account information is accessible as business records.[27]

B. Cryptocurrency Transactions Are Anonymous and Publicly Recorded in a Permanent Digital Ledger by Function of the Blockchain

In cryptocurrency transactions, there are three components in a given entry input to the blockchain ledger: the transaction amount, the proof that the sender has the ability to send that amount, and the recipient's address.[28] Transactions occur on the blockchain through the use of a private and public key.[29] The private key is essentially a signature that is known only to the user that allows a cryptocurrency transaction to initiate; it allows a user to send cryptocurrency to another user.[30] The sender creates a transaction, signs the transaction, and broadcasts it "to the network for validation."[31] Nodes then "verif[y] that indeed your private key corresponds to the provided public key" and confirm the transaction.[32] The public key has a mathematical relationship to the private key, such that proof of ownership of the public key can be

[25] *See id.*

[26] *See* Longman, *supra* note 14, at 121-22.

[27] *See* Jake Frankenfield, *Bitcoin Exchange*, INVESTOPEDIA (Aug. 9, 2021), https://www.investopedia.com/terms/b/bitcoin-exchange.asp [https://perma.cc/V96D-SPAA]; *see also What's a Bitcoin Exchange?*, BITCOIN.COM https://www.bitcoin.com/get-started/how-bitcoin-exchange-works/#2 (describing the "custodial" nature of cryptocurrency transactions on exchange platforms like Coinbase) [https://perma.cc/2S9R-PERY].

[28] *See* Noelle Acheson et al., *How Do Bitcoin Transactions Work?*, COINDESK (Aug. 20, 2013), https://www.coindesk.com/learn/how-do-bitcoin-transactions-work-2/ [https://perma.cc/KTM7-9LUJ]; *see also How Do Bitcoin Transactions Work?*, BITCOIN.COM, https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/ [https://perma.cc/8JLF-48J9].

[29] *See* Zheng et al., *supra* note 18, at 356.

[30] *See* Jake Frankenfield, *Public Key*, INVESTOPEDIA (June 24, 2021), https://www.investopedia.com/terms/p/public-key.asp [https://perma.cc/GZR8-F9PC].

[31] *See* Noelle Acheson et al., *How Do Bitcoin Transactions Work?*, COINDESK (Aug. 20, 2013), https://www.coindesk.com/learn/how-do-bitcoin-transactions-work-2/ [https://perma.cc/KTM7-9LUJ]; *see also How Do Bitcoin Transactions Work?*, BITCOIN.COM, https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/ [https://perma.cc/8JLF-48J9].

[32] *See* Noelle Acheson et al., *How Do Bitcoin Transactions Work?*, COINDESK (Aug. 20, 2013), https://www.coindesk.com/learn/how-do-bitcoin-transactions-work-2/ [https://perma.cc/KTM7-9LUJ]; *see also How Do Bitcoin Transactions Work?*, BITCOIN.COM, https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/ [https://perma.cc/8JLF-48J9].

revealed without revealing the private key.[33] The public key is converted into hash code which is a visible public address entered as a component of the ledger entry.[34] The scrambled sender address combined with the recipient's public key allows the transaction to proceed, and the entry is added to the blockchain where it is visible to everyone with access.[35] In the realm of cryptocurrency exchanges, Coinbase is a broker and holds its own private keys and maintains a database allocating transactions to its users; as such, a Coinbase user does not possess actual private keys for use of transacting on the blockchain.[36]

Whether a user is using Coinbase or a decentralized blockchain directly, they are not relaying their identity during a transaction.[37] A cryptocurrency exchange functions like a stock or commodities market, and the exchange essentially fulfills a buy or sell order for a certain amount.[38] The transaction is also functionally anonymous between buyer and seller, but the cryptocurrency exchange is subject to Know Your Customer (KYC) laws that require the exchange to maintain personally identifiable information about its customers.[39] All that is traded is currency for currency: BTC for USD.[40] The operations are distinct from when users of an exchange then take their cryptocurrency holdings and transact them as payment for a good or service with a seller on a public blockchain.[41] This money can be transferred from the exchange held wallet to a seller, to a different exchange, or to a different type of wallet: online or offline where KYC laws might be different.[42]

C. *A Cryptocurrency Exchange is a Third-Party Broker*

A cryptocurrency exchange is an entity which issues exchange accounts to users who then buy and sell cryptocurrency on the blockchain using the exchange as a "broker" to make those trades.[43] A third-party operated cryptocurrency exchange is not the most ideal use case of blockchain

[33] *See* Jake Frankenfield, *Private Key*, INVESTOPEDIA (Nov. 27, 2021), https://www.investopedia.com/terms/p/private-key.asp [https://perma.cc/DWU6-3LJ7].

[34] *See* Frankenfield, *supra* note 30.

[35] *See* Longman, *supra* note 14, at 121.

[36] *See Data Privacy at Coinbase*, COINBASE, https://help.coinbase.com/en/coinbase/privacy-and-security/data-privacy/what-is-the-gdpr (last visited Feb. 27, 2021); *What Is a Private Key?*, COINBASE, https://www.coinbase.com/learn/crypto-basics/what-is-a-private-key (last visited Apr. 3, 2021).

[37] *See* Frankenfield, *supra* note 30.

[38] *See generally What's the Difference Between Coinbase.com and Coinbase Wallet?*, *supra* note 7.

[39] *See* Longman, *supra* note 14, at 120; *see also* Newby & Razmazma, *supra* note 13.

[40] *See generally What's the Difference Between Coinbase.com and Coinbase Wallet?*, *supra* note 7.

[41] *See* Toshendra Kumar Sharma, *Five Differences Between an Exchange and a Blockchain*, BLOCKCHAIN COUNCIL, https://www.blockchain-council.org/blockchain/five-differences-between-an-exchange-and-a-blockchain/ [https://perma.cc/ERV9-PVTN].

[42] *See* Newby & Razmazma, *supra* note 13.

[43] *What's the Difference Between Coinbase.com and Coinbase Wallet?*, *supra* note 7.

technology.[44] Blockchain was designed to do away with third parties, but one needs technological wherewithal to transact on the blockchain without the help of an intermediary.[45] In this sense, exchanges fill that technological void, and help bring blockchain directly to consumers. Coinbase.com states that its role is as a "cryptocurrency brokerage where you buy or sell cryptocurrency in exchange for fiat currency."[46] While using the exchange, individuals can trade fiat currency like the USD for cryptocurrency or make trades between cryptocurrencies.[47] When an individual opens an account with an exchange, they share private data with the exchange, which implicitly links their personal account data to every transaction executed using the exchange.[48]

In addition, the user's public and private keys are not owned by the user, but by the cryptocurrency exchange.[49] Because of this lack of ownership, a user of an exchange account technically does not even own the cryptocurrency held on their account.[50] A cryptocurrency exchange can be one of many ways that cryptocurrency holders transact in cryptocurrency and keep their cryptocurrency holdings.[51] If someone holds their cryptocurrency on the exchange, the ownership interest is not clear since the exchanges are third-party intermediaries that maintain ownership of the wallet keys to users' private exchange accounts.[52] As financial institutions, cryptocurrency exchanges have responsibilities under the Bank Secrecy Act to collect certain forms of data, create reports on suspicious behavior, and to turn over suspicious information to law enforcement or the government.[53] Additionally, in order to access account data held by a cryptocurrency exchange, law enforcement only needs to obtain a court order or subpoena rather than a search warrant based on probable cause.[54]

[44] *See* Cassiopeia Services, *Challenges and Issues in Cryptocurrency Trading: Beyond the Controversies*, MEDIUM (Feb. 28, 2019), https://cassiopeiaservicesltd.medium.com/challenges-and-issues-in-cryptocurrency-trading-beyond-the-controversies-12bebb7c3849 (the centralization of risk in cryptocurrency exchanges works against the broader goals of decentralization).

[45] *See* United States v. Gratkowski, 964 F.3d 307, 312-13 (5th Cir. 2020).

[46] *What's the Difference Between Coinbase.com and Coinbase Wallet?*, *supra* note 7.

[47] *See* Frankenfield, *supra* note 27; *see also* James Chen, *Fiat Money*, INVESTOPEDIA (Oct. 26, 2021), https://www.investopedia.com/terms/f/fiatmoney.asp (Fiat is currency that is backed by the issuing government rather than a physical commodity) [https://perma.cc/F6Z4-DH7R].

[48] *See* Longman, *supra* note 14, at 132-33.

[49] Cryptopedia Staff, *What Are Public and Private Keys?*, CRYPTOPEDIA, (Sept. 8, 2021), https://www.gemini.com/cryptopedia/public-private-keys-cryptography#section-where-are-my-private-keys [https://perma.cc/5TNT-2QTH].

[50] *See Gratkowski*, 964 F.3d at 312; *see* Cryptopedia Staff, *supra* note 49.

[51] *See generally* Paxful Team, *What Is a Paper Wallet?*, PAXFUL: BLOG (May 27, 2020), https://paxful.com/blog/bitcoin-paper-wallet/ [https://perma.cc/HBT3-PVHD].

[52] *See* Cryptopedia Staff, *supra* note 49.

[53] *See* Christopher Lloyd, *The Privacy Revolution Begins: Did* Carpenter *Just Give Bitcoin Users a Chance to Strike Down the Bank Secrecy Act?*, 88 GEO. WASH. L. REV. 204, 215-16 (2020).

[54] *Id.* at 217.

III. THE CHAIN OF PRIVACY LAW: FROM MAILBOXES TO CRYPTOCURRENCY EXCHANGES

This section describes the purpose of the Fourth Amendment, early Fourth Amendment case law, and how the third-party doctrine evolved when individuals claimed a privacy interest in data held by third parties. This section also presents the modern application of the third-party doctrine in emerging technology cases as well as recent case law assessing the third-party doctrine's application to cryptocurrency exchanges.

A. The Foundation of the Fourth Amendment and Evolution of the Third-Party Doctrine

The Fourth Amendment protects the rights of citizens to keep certain information private and away from the government.[55] Early Fourth Amendment jurisprudence drew distinctions between information that was voluntarily revealed to the public, and information that was kept private.[56] This evolution eventually created the standard conveyed in the third-party doctrine which limits privacy expectations when an individual voluntarily shares information with a third party.[57]

The Fourth Amendment is the grounding principle when determining circumstances under which the state can access private transactional information.[58] The Fourth Amendment states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[59]

The Fourth Amendment was born out of a skepticism and dislike of the British government's use of the general warrant in obtaining access to houses, papers, and effects through search and seizure.[60] The general warrant required a low bar for access, and the result was "unreasonable searches and seizures."[61] The Fourth Amendment departed from this standard by requiring a "probable cause" showing before issuing a warrant.[62]

[55] *See* Ex parte Jackson, 96 U.S. 727, 733 (1877) (the information at issue being sealed letters).

[56] *See id.*

[57] *See* United States v. Miller, 425 U.S. 435, 443 (1976).

[58] *Id.* at 444.

[59] U.S. CONST. amend. IV.

[60] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

[61] Paul Belonick, *Transparency is the New Privacy: Blockchain's Challenge for the Fourth Amendment*, 23 STAN. TECHNOLOGY L. REV. 114, 169 n.345 (2020).

[62] *Id.* at 180.

Early Fourth Amendment jurisprudence attempted to define how the amendment applied in settings involving searches and seizures.[63] In *Ex parte Jackson,* the Court articulated a standard for search and seizure when it came to letters, creating a distinction between content and envelope, specifically that the envelope contained address and directional information, and that content information was the letter within.[64] The content inside was protected from search and seizure, and the address information outside of the envelope did not have the same protections because it was necessary for transferring the letter.[65] Later on, *Katz v. U.S.* fleshed out the "unreasonable" element in the Fourth Amendment test by articulating a "reasonable expectation of privacy" in Fourth Amendment analysis, meaning that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[66] This expectation of privacy test affirms that there may be things revealed to the public in which one retains a privacy right.[67]

The development of the third-party doctrine followed *Katz* and was first articulated in *U.S. v. Miller*, a case concerning whether a bank client had a privacy interest in his checks used at a banking institution; the Court held that checks are "negotiable instruments" used in business, and the customer assumes the risk of having that information shared by engaging in the transaction.[68] The Court mentioned that:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to the Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[69]

This means that when conducting personal business with a bank, a client has no "expectation of privacy" in that data.[70]

[63] *See* Ex parte Jackson, 96 U.S. 727, 733 (1877); *see e.g.*, Belonick, *supra* note 61, at 151-53.

[64] *See Jackson*, 96 U.S. at 732-33.

[65] *See* DANIEL SOLOVE, NOTHING TO HIDE 94 (2011) (explaining generally how secrecy is equated with privacy and defining this as the "secrecy paradigm"); *see, e.g.*, Belonick, *supra* note 61, at 148-51 (Belonick presents the "content/noncontent" and "inside/outside" distinctions in relation to letters and more broadly that the "inside" and "content" of materials is where the privacy interest lies).

[66] Katz v. United States, 389 U.S. 347, 360-61 (1967).

[67] *See id.* at 351-52.

[68] United States v. Miller, 425 U.S. 435, 442-43 (1976).

[69] *Id.* at 443.

[70] *Id.* at 449.

Smith v. Maryland used this same "expectation of privacy" test in the context of pen registers.[71] Pen registers collect a record of the phone numbers being dialed between lines, but they are not able to pick up the content of the calls being tracked.[72] Phone companies maintain the records of these calls, so an individual does not have any real control over this data collection.[73] *Smith* held that because the content of the communications on the phone call was not at issue there is no expectation of privacy in the log of calls created by the pen register and thus a warrant was not needed for law enforcement to obtain the data.[74]

These two cases reaffirm the standard for third-party transactions specifying that there is no reasonable expectation of privacy in information voluntarily shared with a third party.[75] This logic has persisted even as third parties have become more abstract and exist only as banking apps and credit cards that appear only tangentially connected to the entities they proceed from.[76] Under this doctrine, the government or law enforcement has much more ease in acquiring information.[77] There is no need for a warrant showing probable cause, only a written request, a court order, or a subpoena—meaning that fewer limitations are placed on the government or law enforcement preventing them from searching and seizing data related to these consumer transactions.[78]

B. *There Is Mixed Treatment of Emerging Technologies Under the Third-Party Doctrine*

The third-party doctrine applies in the realm of credit cards: cases have held that that there is no reasonable expectation of privacy in a credit card number.[79] However, in the realm of developing technologies, the Supreme Court has applied the third-party doctrine and the Fourth Amendment warrant requirement with different results.[80] In *U.S. v. Jones*, a case concerning

[71] Smith v. Maryland, 442 U.S. 735, 740-41 (1979). A pen register is a "device or process that traces outgoing signals from a specific phone or computer to their destination . . . [and] produces a list of the phone numbers or Internet addresses contacted, but does not include substantive information transmitted by the signals." *Pen Register*, CORNELL L. SCH: LEGAL INFO. INST., https://www.law.cornell.edu/wex/pen_register [https://perma.cc/QF6Q-SVSG].

[72] *Smith*, 442 U.S. at 741.

[73] *Id.* at 742.

[74] *Id.* at 741, 745-46.

[75] *See generally id.*; *Miller*, 425 U.S. at 442-44.

[76] *See* United States. v. Medina, No. 09-20717-CR, 2009 WL 3669636, at *11 (S.D. Fla. Oct. 24, 2009); United States v. DE L'Isle, 825 F.3d 426, 432 (8th Cir. 2016).

[77] *See* Margaret E. Twomey, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 MICH. TELECOMM. & TECHNOLOGY L. REV. 401, 402 (2015); Lloyd, *supra* note 53, at 217.

[78] Lloyd, *supra* note 53, at 217.

[79] *See Medina*, 2009 WL 3669636 at *11 ("the credit card holder voluntarily turns over his credit card number every time he uses the card"); *DE L'Isle*, 825 F.3d at 432 ("when the holder uses the card he 'knowingly disclose[s] the information on the magnetic strip of his credit card to a third party and cannot claim a reasonable expectation of privacy in it'").

[80] *See generally* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

whether the attachment of a GPS device on a vehicle constituted a search or seizure, Justice Sotomayor concurred that it might be time to reconsider the third-party doctrine since the digital age involves so much information-sharing with third parties.[81] Similarly, in *Kyllo v. U.S.*, when thermal heat imaging had been used to obtain a warrant to observe a potential illegal marijuana operation, the Court held that the warrant was improperly obtained as the home was a basic constitutionally protected area and that "advancing technology" that invades such a constitutionally protected area needs to be regarded carefully regardless of whether "intimate details" are revealed.[82]

In a recent Supreme Court case, *U.S. v. Carpenter*, the Court considered whether or not there was an expectation of privacy in cell site location information (CSLI) data revealing thousands of location points for a criminal defendant; the Court then assessed the third-party doctrine in connection with this data.[83] *Carpenter* assesses the privacy interest in CSLI data by looking at two different lines of case law: that of *Katz* and the "expectation of privacy in his physical location and movements" and one's "expectation of privacy in information voluntarily turned over to third parties."[84]

Carpenter hearkens back to *Miller* in order to make a distinction that the CSLI data was different than the "business records of the banks" at issue in *Miller*.[85] CSLI data reveals a cell phone's approximate position in relation to nearby cell phone towers, and, in this case, the location was revealed thousands of times and was acquired by law enforcement without a search warrant.[86] The technology at issue in *Carpenter* was the cell phone's periodic and innate attempts to establish signal connection by connecting to cell phone towers and the data trail created—CSLI data.[87] CSLI is data that is revealed about a cell phone's approximate position in relation to nearby cell phone towers; GPS data on a cell phone is even more specific, tracking location down to a 5–10-foot range.[88] This type of data implicates third-party cell phone companies or providers of GPS services.[89] This near-constant search for cell towers created a data trail identifying all of the towers that were near defendant's movements on the night the crime was committed.[90] The business records discussed in *Miller* are significantly different than the GPS-like tracking that occurred in *Carpenter*.[91] The *Carpenter* Court held that the tracking of someone's movements in this way without any voluntary action

[81] *Jones*, 565 U.S. at 417.

[82] Kyllo v. United States, 533 U.S. 27, 28 (2001).

[83] *Carpenter*, 138 S. Ct. at 2208-09.

[84] *Id.* at 2209-10, 2214-15.

[85] *Id.* at 2216.

[86] *Id.* at 2209, 2225.

[87] *Id.* at 2210.

[88] CELL PHONE LOCATION TRACKING, A NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS (NACDL) PRIMER (2016) https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf [https://perma.cc/U554-NREM].

[89] *Id.*

[90] *See Carpenter*, 138 S. Ct. at 2208-09.

[91] *See id.* at 2209 (CLSI data is "detailed, encyclopedic, and effortlessly compiled").

taken by the cell phone user seemed to be an overstretch of this "voluntary" element contained in the logic of the third-party doctrine.[92]

The *Carpenter* Court then assessed voluntary disclosure as it was described in *Smith*, in which bank records voluntarily shared between a bank client and the bank were considered business records.[93] A key touchstone for finding that the third-party doctrine applied in *Smith* was because of the client's voluntary handing over of information.[94] In *Carpenter*, the Court posited that while an individual may voluntarily use their cell phone, the cell phone user is not voluntarily relaying location data to third-party cell phone companies because it occurs involuntarily as a function of the technology.[95] The Court held that the third-party doctrine was over-extended when law enforcement acquired CSLI data without a warrant and connected the defendant to the crime.[96]

C. *Cryptocurrency Exchanges Are Third Parties in the Context of the Third-Party Doctrine*

Based on recent caselaw, cryptocurrency exchanges are third parties under the Fourth Amendment for purposes of the third-party doctrine. *Zietzke v. U.S.* is a blockchain case from the Northern District of California concerning personal information shared with the Coinbase cryptocurrency exchange that was tied to an accountholder who had inaccurately reported cryptocurrency gains on tax returns.[97] The *Zietzke* court held that consumers revealing information to Coinbase was comparable to the *Miller* holding concerning bank records, and thus, law enforcement rightfully did not need to obtain a warrant.[98]

U.S. v. Gratkowski presented a similar issue in which law enforcement subpoenaed Coinbase, and obtained access to Gratkowski's account without a warrant.[99] At issue was a blockchain in which a cluster of Bitcoin addresses were found to be connected with a child pornography website.[100] Federal agents recruited a service to analyze the cluster of addresses to identify specific ones connected with the website.[101] After identifying the implicated

[92] *Id.* at 2216-18 (*Carpenter* Court describing cell phones as practically a fixture of the human "anatomy").

[93] *Id.* at 2219-20.

[94] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[95] *Carpenter*, 138 S. Ct. at 2220.

[96] *Id.* at 2220, 2223 (While the Court described the holding as "narrow," the narrowness of this holding seemed to stem from the fact that cell phones are indispensable in modern society and that CSLI data is not voluntarily shared, but a virtue of the cell phone's operation. The narrowness of this holding likely would not preempt a similar logic being applied to other privacy-invasive technologies).

[97] Zietzke v. United States, No. 19-cv-03761-HSG (SK), 2020 WL 264394, at *1 (N.D. Cal. Jan. 17, 2020).

[98] *Id.* at *13 (because this information shared by Zietzke was "voluntarily exposed . . . to Coinbase for commercial purposes, he does not retain a reasonable expectation of privacy over this information").

[99] United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020).

[100] *Id.*

[101] *Id.*

addresses, the agents served a "grand jury subpoena on Coinbase—rather than seeking and obtaining a warrant—for all information relating to the Coinbase customers whose accounts had sent Bitcoin to any of the addresses" included in the cluster.[102] The agents did not have any identifying information concerning the customers whose addresses they were seeking via subpoena.[103] However, the Fifth Circuit held that because "every Bitcoin user has access to the public Bitcoin blockchain and can see every Bitcoin address and its respective transfers" Gratkowski had no privacy interest.[104] In its analysis, the court stated that those people who interact on the blockchain have more privacy "than those who use other money-transfer means" because the blockchain provides more privacy than a bank.[105] However, this "privacy" seems more arbitrary than actual, considering that once law enforcement has the address of a blockchain user, the blockchain can be traced back to a cryptocurrency exchange, and the user seems to be treated no differently than "those who use other money-transfer means."[106]

Likewise, the *Gratkowski* court does not apply *Carpenter*, noting that Coinbase records are "limited" and do not create the same potential for constant surveillance as do the CSLI data; as well as the fact that transacting on Coinbase requires an "affirmative act" from users, more akin to that which was at issue in *Miller*.[107] To further flesh out what expectation of privacy users have in their data on Coinbase, the court assesses Coinbase in light of *Miller* and the requirements that Coinbase must follow under the Bank Secrecy Act.[108] The key distinction that the Fifth Circuit leaves us with is that people who choose Coinbase (a third-party money transmitter), rather than just going directly to the blockchain without an intermediary, end up sacrificing their privacy in the same way that consumers sacrifice their privacy interest when transacting with a bank.[109]

IV. A NECESSARY DISTINCTION: THE PROBLEM OF CONFLATING THE PUBLIC BLOCKCHAIN WITH THIRD-PARTY CRYPTOCURRENCY EXCHANGES.

As courts are presented with issues concerning the third-party doctrine's application to blockchain transactional data, there is a need to recognize the distinction between the blockchain and a cryptocurrency exchange. Part IV, Section A assesses why *Carpenter* can be looked at as establishing a new precedent concerning how courts examine the third-party

[102] *Id.*

[103] *No Search Warrant Required for Records of Bitcoin Transactions, the Fifth Circuit Holds*, JONES DAY, (June 2020) https://www.jonesday.com/en/insights/2020/07/no-search-warrant-required-for-records-of-bitcoin-transactions-the-fifth-circuit-holds [https://perma.cc/KNV7-LYC9].

[104] *Gratkowski*, 964 F.3d at 312.

[105] *Id.*

[106] *See id.*

[107] *Id.* at 312.

[108] *Id.*

[109] *Id.* at 312-13.

doctrine's application in emerging technology cases. Section B identifies the issue with conflating the public ledger blockchain transactions as a public revelation of identity and proposes how a cryptocurrency exchange is distinct and should be approached by law enforcement with this in mind. Finally, Section C expands on Section B by discussing specific case law and recommends why the search warrant should be required.

A. *Cryptocurrency Exchanges Are Third Parties, but Carpenter Sets New Precedent for Finding a Privacy Interest when Emerging Technologies Involve Third-Party Transactions*

Under the third-party doctrine, cryptocurrency exchange users do not currently have a recognized privacy right to their stored data because the exchanges are viewed as money transmitters.[110] However, the two case lines presented in *Carpenter* provide a basis for recognizing an independent privacy interest in blockchain data. This section asserts that the logic of *Carpenter* justifies finding a privacy interest in blockchain data even while cryptocurrency exchanges are considered third parties.

The *Carpenter* Court stated that it keeps "[f]ounding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools."[111] As evidenced in *Gratkowski*, blockchain transactions require innovative surveillance tools to uncover malicious behavior.[112] Law enforcement cannot simply open up a blockchain ledger and do a quick "Control+F" search to find a public key; this requires cryptography and careful analysis of the blockchain to discern information such as the transaction ID, IP address, or geographic locational data for a suspect's Virtual Asset Service Provider.[113] The catalogues of information that can be dredged up in blockchain transactions are not unlike the CSLI data in *Carpenter* or law enforcement's use of a heat detector in *Kyllo* to uncover marijuana possession.[114] In *Kyllo* and *Carpenter*, these intrusions were held as violations of a person's reasonable expectation of privacy.[115]

In *Carpenter*, the court focused on how the reasonable expectation of privacy in CSLI data was at "the intersection of two lines of cases . . . [One] set . . . addresses a person's expectation of privacy in his physical location

[110] *Money Transmitter Licensing for U.S. Crypto Companies*, KELMAN LAW, (July 13, 2020), https://kelman.law/insights/money-transmitter-licensing-for-u-s-crypto-companies/ (describing the regulation of cryptocurrency exchanges as money transmitters) [https://perma.cc/KD76-5JRS]; Lloyd, *supra* note 53, at 214-15 (noting the potential for *Carpenter* to effect blockchain regulation).

[111] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

[112] *See Gratkowski*, 964 F.3d at 309.

[113] Lucas Ropek, *Cryptocurrency Tracer Could Give Cops an Edge on Cybercrime*, GOV'T TECHNOLOGY, (Sept. 22, 2020), https://www.govtech.com/security/cryptocurrency-tracer-could-give-cops-an-edge-on-cybercrime.html (a virtual asset provider is "the forum through which cryptocurrency can be translated into actual cash") [https://perma.cc/9QP3-AZYH].

[114] *See Carpenter*, 138 S. Ct. at 2216-17; Kyllo v. United States, 533 U.S. 27, 34-35 (2001); *see, e.g.*, Longman, *supra* note 14, at 132.

[115] *See Carpenter*, 138 S. Ct. at 2216-17; *Kyllo*, 533 U.S. at 34-35.

and movements" while the other asserts that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[116] Concerning the expectation of privacy in physical location and movements, the CSLI data is "detailed, encyclopedic, and effortlessly compiled."[117] While *Carpenter* was, by its terms, "a narrow decision," the Court's logic acknowledged how new challenges presented by developing technologies invite caution about the rigid application of the third-party doctrine; these limitations of the third-party doctrine cannot reasonably be confined to CSLI data.[118] The tracking of physical movements may be troubling, but equally troubling is the tracking and ability to trace any data movement that reveals intimate content about the nature of transactions that individuals engage in.[119] On the blockchain, each transaction reveals a user's public key, and the public ledger reveals the chronological history of the user's transactions.[120] In creating an exception for CSLI data, the Court in *Carpenter* was focused on the fact that the "individual continuously reveals his location to his wireless carrier implicat[ing] the third-party principle of *Smith* and *Miller*."[121] This same logic could be applied to blockchain transactions completed through cryptocurrency exchanges because even while a cryptocurrency exchange maintains and owns the public and private keys associated with accounts hosted by their service, this continuous stream of data transactions listed on the blockchain is not the same as a bank possessing transaction history from individual clients.[122] A cryptocurrency exchange is essentially a public marketplace; it only facilitates what people can do by themselves if they remove themselves to a decentralized blockchain.[123] This distinct separation between the entity of the blockchain and the cryptocurrency exchange suggests that courts acknowledge that there is a separate privacy interest in blockchain data that is reflected by the lack of ownership in what is publicly viewable on the ledger and what is owned by the third-party cryptocurrency exchange.

Additionally, the *Carpenter* Court addresses the voluntariness of data sharing.[124] The two main points addressed are (1) how cell phones are pervasive and are essentially anatomical extensions in the modern world, and (2) that the cell phone's ability to connect to a cell tower does not require any

[116] *Carpenter*, 138 S. Ct. at 2214-16 (quoting *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)).

[117] *Id.*

[118] *Id.* at 2214, 2220.

[119] Longman, *supra* note 14, at 132.

[120] Rui Zhang, et al., *Security and Privacy on Blockchain*, 52 ASS'N FOR COMPUTING MACHINERY COMPUTING SURVS. 51:2-3 (July 2019) (the "consensus procedure . . . enforced by the network . . . controls . . . the admission of new blocks into the block chain" and ensures the validity of each block).

[121] *Carpenter*, 138 S. Ct. at 2209.

[122] *See* Frankenfield, *supra* note 27; *see also What's a Bitcoin Exchange?*, *supra* note 27 (describing the "custodial" nature of cryptocurrency transactions on exchange platforms like Coinbase).

[123] *See* Frankenfield, *supra* note 27; *see What's a Bitcoin Exchange?*, *supra* note 27.

[124] *Carpenter*, 138 S. Ct. at 2220.

voluntary action from the user.[125] Certainly, blockchain technology is not so pervasive that it is a "feature of human anatomy."[126] However, the verification of a transaction requires no affirmative act on behalf of the user: it is a function of the program.[127] This "voluntariness" factor that the Court weighs is conspicuously absent from a blockchain transaction; courts assessing claims that blockchain follow a *Carpenter* analysis should not so easily dismiss *Carpenter*'s application based on the fact that the data being shared is financial in nature and that the blockchain is not as ubiquitous as a cell phone.[128] The reality is that once one consents to use a cryptocurrency exchange to transact, there is no voluntariness in the data sharing at all: it is required for individuals to submit to KYC protocols and share personally identifiable information with the platform in order to even open an account.[129]

The holding of *Carpenter* states that a warrant requiring probable cause was required to obtain CSLI records.[130] The Court's analysis should not be read to exclude a scenario in which blockchain technology appropriately fits within the Fourth Amendment's protection even while a cryptocurrency exchange is a third party. Even if not explicitly fleshed out in the opinion, the canon of construction concerning avoidance of absurd results in assessing advancing technology appears to undergird the logic of the opinion, and this principle is what should guide future courts in analyzing blockchain technology in these circumstances.[131] In *Carpenter*, there is a focus on the Court's role to preserve the Fourth Amendment's protection where technology is advancing. If the Court is ready to protect the public location of individuals as CSLI data under the Fourth Amendment, the issue of whether to consider the time-stamped, immutable blockchain transactional data as worthy of protection is ripe for consideration as well.

B. *Why the Ledger's Transparency Does Not Negate the Privacy of Actors Using a Third-Party Exchange*

Blockchain promises to deliver privacy while remaining transparent.[132] Privacy law is largely governed by a framework that relies on the concealment of information in order to maintain privacy, a concept that does not seem to line up with the transparency of the blockchain.[133] This premise that secrecy and privacy are one and the same arises frequently in the application of the third-party doctrine.[134] The hallmark case, *Smith*, talks about the concept of secrecy in privacy analysis: "it is too much to believe that telephone

[125] *Id.* at 2218, 2220.

[126] *Id.* at 2218.

[127] Zhang, et al., *supra* note 120, at 51:3.

[128] *See* United States v. Gratkowski, 964 F.3d 307, 312-13 (5th Cir. 2020).

[129] *See What Is AML/KYC in Crypto?*, SYGNA: BLOG , https://www.sygna.io/blog/what-is-aml-kyc-in-crypto/ [https://perma.cc/4JS9-49YH].

[130] *E.g.*, *Carpenter*, 138 S. Ct. at 2221.

[131] *Id.* at 2214, 2216-17.

[132] *See* Longman, *supra* note 14, at 118-19; *see also* Belonick, *supra* note 61, at 118-19.

[133] SOLOVE, *supra* note 65, at 94; *see also* Belonick, *supra* note 61, at 114-15.

[134] Belonick, *supra* note 61, at 122.

subscribers . . . harbor any general expectation that the numbers they dial will remain secret."[135] Some have questioned why someone with nothing to hide would be worried about their privacy on the blockchain where everything is recorded publicly. The answer should be clear: privacy's end goal does not have to be secrecy, and with blockchain, secrecy is not the end goal.[136] Blockchain's end goal is to "remove secrecy while maintaining privacy."[137]

There is a need to acknowledge that public ledger blockchain transactions are not a public revelation of identity; identity remains secret when the transaction is posted. A cryptocurrency exchange possesses private information obtained by KYC—information which is distinct from the public revelations on the blockchain ledger, and it should be approached by law enforcement with this in mind. By changing the conversation in this way, we are simply looking back to the foundation of Fourth Amendment law.[138] Early Americans wanted to secure their possessions from unfair intrusion.[139] These possessions were enumerated in the provision, but that provision did not include an exemption for those papers and records that were shared with others.[140] In the blockchain, the identity of individuals is concealed—the transactions only reveal the addresses of the users.[141] Paul Belonick describes this as a content/noncontent distinction and compares blockchain transactions to phone call records in a pen register; he describes how, traditionally, a pen register would record the phone number of a caller (the phone number being noncontent information), but that none of the contents of the call are recorded in the register. [142] Conversely, the blockchain reveals the contents of the transaction on the blockchain, without fully disclosing the content of the identity of the user who posted the transaction.[143] In *Katz*, the pen register case, the Court held that the individual standing in the phone booth had a reasonable expectation of privacy in the content of his conversation.[144] This content distinction should remain important in Fourth Amendment analysis and should be the basis for finding a privacy interest in the hidden content of a user's identity.[145]

We have been willing to recognize privacy interests in things exposed to the public based on a reasonable expectation of privacy.[146] The fact that law enforcement relies on the third-party doctrine to access content information at a lower standard than a search warrant is worrisome, as the Fourth Amendment has been neutered of any real meaning in an age that depends on third-party transactions.[147] If content truly is the basis of

[135] Smith v. Maryland, 442 U.S. 735, 743 (1979).

[136] Belonick, *supra* note 61, at 153.

[137] Longman, *supra* note 14, at 127.

[138] Belonick, *supra* note 61, at 158.

[139] *Id.*

[140] *Id.* at 158, 166.

[141] Longman, *supra* note 14, at 122.

[142] *See* Belonick, *supra* note 61, at 152.

[143] *See id.* at 153.

[144] Katz v. United States, 389 U.S. 347, 353 (1964).

[145] Belonick, *supra* note 61, at 151-53.

[146] *Katz,* 389 U.S. at 351, 360-61.

[147] United States v. Jones, 565 U.S. 400, 417-18 (2012) (Sotomayor, J., concurring).

protection, then blockchain data should be assessed with this standard.[148] This standard would not mean that we ignore the fact that the public ledger contains public key information that can be identified, but it does mean that we recognize that no investigator is going to be able to independently find out the user's identity when presented with just a string of digits. When an investigator has identified a public key, law enforcement should then be required to obtain a search warrant, because at that specific moment in time, they have no lead on identity. The only identity that should be searched for when presenting a cryptocurrency exchange with a search warrant is the identity associated with that public key.

C. Law Enforcement Should Need Search Warrant to Obtain Personal Information Held by a Cryptocurrency Exchange

The blockchain, unlike banks and phone companies, is not a third-party intermediary, and the transactions are not part of the course of business of a cryptocurrency exchange: it is a ledger establishing a public record of transactions. At issue in *Miller* were bank records, and the Court held that because these records were property of the bank, Miller had no privacy interest.[149] At issue in *Smith* was the expectation of privacy in the phone numbers dialed and traced by the pen register.[150] The phone company, possessing records of the phone calls placed by those using the service, is a third party who has "legitimate business purposes" in maintaining this data, just like the bank in *Miller*.[151]

In *Miller*, the bank was subpoenaed based on a tip that two individuals were connected to an illegal distillery trade, and, in *Smith*, the police did not get a warrant or court order, but merely requested the phone company install a pen register. [152] In either scenario, under the third-party doctrine, the third parties were not issued a warrant, but still turned over information in their possession: in the first case, there was no need for a warrant because there was no Fourth Amendment interest in the data, in the second case, the Court held that there was no content information, thus no Fourth Amendment violation in obtaining the records.[153]

On the surface, the fact pattern in *Gratkowski* resembles that of *Miller*. However, what is at issue in *Gratkowski* is that federal law enforcement was able to identify a cluster of likely addresses that comprised a pornography website, but had no leads on any customers.[154] Because there was no requirement for a search warrant, it did not matter whether the evidence that the officers had collected regarding the cluster of addresses was enough to establish probable cause that certain addresses were associated with a known pornography website: all they needed was a subpoena to obtain the

[148] *See* Belonick, *supra* note 61, at 151-53.

[149] United States v. Miller, 425 U.S. 435, 439-40 (1976).

[150] Smith v. Maryland, 442 U.S. 735, 742 (1979).

[151] *Id.* at 742-44.

[152] *See Miller*, 425 U.S. at 435-37; *Smith*, 442 U.S. at 735.

[153] *See Miller*, 425 U.S. at 435-37; *Smith*, 442 U.S. at 735.

[154] United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020).

cryptocurrency exchange account information of unknown addresses who had transacted with the address cluster.[155] If a search warrant had been the standard, they should have identified the public key addresses beforehand to see if Coinbase had public keys associated with any publicly available transaction information rather that subpoenaing Coinbase for account holder information and implicating an unknown amount of Coinbase customers in their search.[156]

Coinbase is a third party which owned at least one account address implicated in trading with a cluster of addresses associated with a criminal website.[157] The application of the third-party doctrine may make sense here if the forensic investigation into the address cluster had actually revealed that the address belonged to Gratkowski, because then law enforcement would be seeking information for an identified customer that Coinbase could confirm. However, even if Gratkowski was an "identified" customer, the forensic investigation by law enforcement only reveals the address, giving no information about customer identity. Gratkowski's account address was revealed during the investigation, but by operating under a subpoena, the evidence concerning the website cluster of addresses was treated akin to a general warrant to access Coinbase records for associated addresses and customer information.[158] In the opinion, the court makes the distinction between a third-party exchange like Coinbase and the blockchain.[159] The court also acknowledged that "users have the option to maintain a high level of privacy by transacting without a third-party intermediary," but the court does not question whether the subpoena was constitutional when law enforcement had no reason to suspect Coinbase accounts had an association with the criminal cluster of addresses prior to Coinbase's acquiescence to the subpoena request.[160] The forensic analysis directed at the blockchain to obtain data about whether certain addresses were part of a suspected child porn trafficking site and the use of that analysis to obtain data that incriminated previously unsuspected individuals reveals how this distinction between the blockchain and the exchange is eroded in *Gratkowski*.[161] The erosion of this distinction appears to be an expansion of the third-party doctrine beyond its prior bounds.[162]

Gratkowski acknowledges that the blockchain ledger is public; the fact that anyone can log on and view the transactions on the Bitcoin ledger may

[155] *Id.*; *see also Probable Cause*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/probable_cause (probable cause can be established when there is "reasonable basis for believing that a crime may have been committed…or when evidence of the crime is present in the place to be searched.") [https://perma.cc/7XSS-J3L9].

[156] *See Gratkowski*, 964 F.3d at 309.

[157] *Gratkowski*, 964 F. 3d at 309.

[158] *Id.*

[159] *Id.* at 309 ("to conduct Bitcoin transactions, Bitcoin users must either download Bitcoin's specialized software or use a virtual currency exchange, such as the one used here, called Coinbase").

[160] *Id.* at 312-13 (this could be accomplished by using software to transact on the blockchain without an exchange, but activity requires sophisticated "technical expertise").

[161] *Id.* at 312-13.

[162] *Id.*

seem to make it redundant to require a search warrant to view what is in plain sight.[163] But these transactions do not relay identity in the way that they reveal public keys.[164] This is evidenced by the fact that law enforcement needed to subpoena Coinbase to even find out which addresses they possessed had transacted with the website.[165] This extensive search for accounts and seizure of information is much different than subpoenaing a bank for a known suspect's bank records or tracing the phone calls of a known suspect with a pen register.[166] The blockchain may contain a recipient's address, but it does not directly reveal any content information about the sender or recipient.[167] Before subpoenaing Coinbase, there was no reasonable suspicion of any individuals in particular; law enforcement should be required to establish probable cause and obtain a warrant to search an exchange service, otherwise this type of search too closely resembles the general warrant, the rejection of which was a key motivator to the drafters of the Fourth Amendment.[168]

The lens of early Fourth Amendment jurisprudence offers further insight into this concern. *Ex parte Jackson* created the logical and theoretical distinction between envelope and content.[169] The court held that the envelope had no privacy interest because it was exposed to the public strictly for the transmission of data.[170] The content inside the envelope retained a privacy interest because it was enclosed from view; the government could not just take any envelope, open it up, and discern its contents.[171] This distinction was a logical extension to protect Americans from general warrants.[172]

If we apply this same logic to the blockchain, we can think of the public keys on the blockchain as equivalent to an address on an envelope.[173] The block in the ledger reveals addresses that engaged in the transaction, but does not establish identity.[174] Conversely, in *Ex parte Jackson*, the address did identify the individual but was also non-content information.[175] Likewise, in the early third-party doctrine cases, the pen register and bank records automatically could be tied to the party who owned the phone number or the

[163] *Id.* at 312.

[164] Longman, *supra* note 14, at 123.

[165] *Gratkowski,* 964 F.3d at 309.

[166] *See* United States v. Miller, 425 U.S. 435, 437 (1976); Smith v. Maryland, 442 U.S. 735, 735 (1979).

[167] Longman, *supra* note 14, at 123; Belonick, *supra* note 61, at 153.

[168] Belonick, *supra* note 61, at 151-53, 170.

[169] *Id.* at 151-53.

[170] *See* Ex parte Jackson, 96 U.S. 727, 732-33 (1877).

[171] *See id.*; *see also* Belonick, *supra* note 61, at 151.

[172] *See* Belonick, *supra* note 61, at 151-52, 162; *Jackson*, 96 U.S. at 732-33.

[173] Belonick, *supra* note 61, at 153, 160-61 ("like a physical address, directing the transaction to a recipient"; it would not make sense to require law enforcement to "avert their gazes" from this observable data); *see also* Riana Pfefferkorn, *Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?,* 49 CONN. L. REV. 1393, 1429-1430 (2017) ("if an encryption key qualifies as content information, then its seizure will typically require a warrant; not so if it is non-content").

[174] Belonick, *supra* note 61, at 153.

[175] *Jackson,* 96 U.S. at 732-33.

bank account, respectively.[176] These distinctions reveal that while blockchain wasn't anticipated by the Fourth Amendment, it still operates within the logic of what the Fourth Amendment was designed to protect.[177] As mentioned by Paul Belonick, this "non-content" data of digits in a blockchain transaction may still preserve a privacy right simply because it cannot be so easily connected to an individual without cryptographic analysis.[178] Subpoenas based on evidence of a collection of addresses should not be the basis to seek out every unknown user who may have transacted with a suspect entity; allowing for this standard as it was established in *Gratkowski* sets a dangerous precedent that diverts from traditional Fourth Amendment jurisprudence.

V. COURTS OR CONGRESS SHOULD RECOGNIZE A PRIVACY INTEREST IN BLOCKCHAIN TRANSACTIONS

This section first presents proposed solutions to the problems enumerated above and then assesses the counterarguments that logically flow from this analysis and proposes solutions.

A. Later Court or Congressional Developments Provide Future Opportunities to Distinguish Exchanges from Blockchain

Blockchain technology should be understood as an advancement in technology that needs to be examined with the same care as technologies in the family of cases that have followed *Miller* and *Smith*.[179] Blockchain transactions are comprised of address information: the identity information possessed by exchanges should not be accessible without probable cause and a warrant since the blockchain does not record this identity information in the public ledger.[180] Formalization of this principle could be achieved either through the courts or by federal legislative action.

1. Courts Should Look at Blockchain as an Emerging Technology, Distinct from Online Banking Apps and Cell Phones

The technical and fact-specific realities of blockchain's function lend themselves easily to comparison with technologies that have been held as too invasive and intrusive to stand without a warrant. It will be critical to

[176] *See* United States v. Miller, 425 U.S. 435, 437 (1976); Smith v. Maryland, 442 U.S. 735, 735 (1979).

[177] Belonick, *supra* note 61, at 151-53.

[178] *Id.* at 153.

[179] *See* Kyllo v. United States, 533 U.S. 27, 35 (2001) (the court resists an approach that "would leave the homeowner at the mercy of advancing technology"); United States v. Jones, 565 U.S. 400, 430-31 (2012) (Alito, J., concurring) (court looks at the reasonable person's expectation of privacy in using new GPS technology); Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (the court talks about the "infallible" memory of the technology at issue in assessing the potential privacy right).

[180] Belonick, *supra* note 61, at 153.

distinguish blockchain from instances of new technologies that have fallen under the third-party doctrine. In *Carpenter*, the Supreme Court found that CSLI data was equally if not more intrusive than the GPS data at issue in *Jones*, when the Supreme Court held that attaching a GPS to a suspect's vehicle violated his right to privacy in his movements; but even more noteworthy was that this type of data was held to not be subject to the third-party doctrine even though it was owned by a third party.[181] If it could be shown that blockchain data is more akin to the content-envelope issue, then it could be argued that the third-party doctrine may not apply even if a third-party exchange claims ownership of the address and public/private keys.[182]

2. Congress Needs to Assess the Gaps Created by the Emergence of New Technology with Legislation Like it Did with the 1978 Right to Financial Privacy Act

In response to the holding in *Miller*, Congress passed the Right to Financial Privacy Act of 1978, which requires "a subpoena, a summons, a search warrant, or the customer's written consent, or . . . the government [to] submit[] a formal written request."[183] This was an attempt to fill the gap in Fourth Amendment protections effectuated by passage of the Bank Secrecy Act and the result of the *Miller* case.[184] Congress is similarly aware of privacy concerns that are only amplified by the free reign given third parties in the digital age.[185] Congress is in the position to reassess the reach of the third-party doctrine in light of the role that third parties play in the digital world, as noted in *Jones*.[186] Such a solution from Congress could be to pass a law that requires law enforcement to establish probable cause concerning implicated addresses before obtaining consumer records from a cryptocurrency exchange.

B. Blockchain Threats to Established Fourth Amendment Jurisprudence and Protecting Privacy in the Face of Criminal Activity

The following two sections assess concerns about whether blockchain threatens to expand *Carpenter*'s supposedly narrow holding, as well as

[181] *Carpenter*, 138 S. Ct. at 2217, 2220.

[182] *E.g.*, Belonick, *supra* note 61, at 151-53.

[183] Longman, *supra* note 14, at 115 (citing *Duncan*, 813 F.2d 1135, 1337 (4th Cir. 1987)).

[184] Longman, *supra* note 14, at 115; Lloyd, *supra* note 53, at 218.

[185] Cameron F. Kerry & John B. Morris, Jr., *Framing a Privacy Right: Legislative Findings for Federal Privacy Legislation*, BROOKINGS INST., (Dec. 8, 2020), https://www.brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/ [https://perma.cc/45WT-NMSM].

[186] *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

broader worries about the effects on criminal prosecution in the cryptocurrency space.

1. *Carpenter* Accommodates Blockchain in Its Analysis: Blockchain Does Not Require Special Protection

While some might argue that the approach proposed in this Note would undermine established case law, this proposal does not apply a special protection or stretch *Carpenter*. Blockchain is a developing technology, just like the technologies assessed in *Carpenter*, *Jones*, and *Kyllo*.[187] As such, it should be recognized that obtaining records in the manner conducted in *Gratkowski* did not comport with typical probable cause requirements under the Fourth Amendment.[188] Law enforcement had no lead on any implicated identities which Coinbase was able to supply.[189] In situations like this, law enforcement should be required to identify individual account addresses in these transactions and use this information to present a search warrant to Coinbase. This two-step procedure would honor the distinction between the actual third-party exchange and the blockchain.

2. Criminals Do Not Evade Liability with this Proposal: The Third-Party Doctrine Should Not Reach Activity Outside a Third-Party's Possession

If we fear technology's negative use cases more than we prize protecting citizens' Fourth Amendment rights, we may risk putting up too many barriers for users to engage in innovations without fear of government overreach. In this regard, blockchain technology creates a space that is different than what was initially at issue when the Bank Secrecy Act was passed and when the third-party doctrine was applied to banks.[190] This legal regime predated the Internet and could not comprehend the digital economy of blockchain. This new world is ripe for a second look at the third-party doctrine, as evidenced in *Carpenter*.[191]

By adopting a willingness to see how third parties are implicated and involved in these transactions, it may open the door to a more honest interpretation and application of the Fourth Amendment in the modern era, as it is made more irrelevant in a world where every transaction seems to implicate a third party. Rather than allowing access of private information possessed by exchanges through a simple subpoena, court order, or written request, the distinction between blockchain and exchanges would be honored

[187] *See Kyllo*, 533 U.S. at 35; *Jones*, 565 U.S. at 430-31 (Alito, J., concurring); *Carpenter*, 138 S. Ct. at 2219.

[188] United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020).

[189] *Id.*

[190] United States v. Miller, 425 U.S. 435, 442-43 (1976).

[191] *Carpenter*, 138 S. Ct. at 2224.

by requiring an actual warrant supported by probable cause for law enforcement seeking information about exchange users.

VI. Conclusion

The third-party doctrine was first asserted in the realm of early technological development with the telephone and in bank records. That era could not anticipate a tech innovation like blockchain technology and the role played by third-party intermediaries controlling data. The protections of the Fourth Amendment and the third-party doctrine are always being tested by the new technologies used to conduct surveillance and communicate. By assessing new technology in light of the Fourth Amendment's purpose, privacy can be protected in the digital age.

This paper has attempted to reveal the concerns raised by courts applying the third-party doctrine to blockchain transactions and to encourage dialogue considering the implications of this technology and why the solutions may not be that different than prior treatment of advancements like GPS and CSLI data. As more companies adopt blockchain, courts should be made aware of the distinction between the blockchain and a third-party exchange's ownership of an address and private data. Consumers should only lose their expectation of privacy in their account information if a properly acquired warrant is brought against an exchange.