# NOTE

# THE PRIVACY LIMITS OF TRANSACTING IN BITCOIN

Yana Kogan*

*The Bitcoin blockchain, a prime example of disruptive technology, has fundamentally altered the way various industries approach remote transactions. Bitcoin grants privacy to its users by anonymizing public keys, provides autonomy by eliminating the need for trusted third parties, and maintains transparency through its public disclosure protocol. Bitcoin is an innovative manifestation of the Fourth Amendment ideals of security and autonomy. It is, thus, no surprise that the Bitcoin blockchain presents unprecedented Fourth Amendment challenges for courts to consider.*

*In United States v. Gratkowski, the Fifth Circuit addressed the novel issue of whether Fourth Amendment protections extend to an individual's Bitcoin transactions. Notably, the court was the first to find that an individual does not have a privacy interest in their information located directly on the Bitcoin blockchain. However, the Fifth Circuit applied inconsistent and flawed reasoning in reaching this decision, demonstrating a fundamental misunderstanding of Bitcoin and its users.*

*Accordingly, this Note argues that the Gratkowski decision should be applied narrowly and with caution, especially considering the Supreme Court's warnings against the incompatibility of current Fourth Amendment doctrine with*

* J.D. 2023, Columbia Law School; B.A. 2019, University of California, Santa Barbara. Many thanks to Professor Zohar Goshen for his assistance in developing this topic. Additional thanks to the editorial board and staff of the *Columbia Business Law Review* for their dedication in preparing this Note for publication. Finally, my sincerest gratitude to my family for their unwavering love and support throughout my academic journey.

*the digital age. It then suggests implementing a modified reasonable-expectation-of-privacy standard, supplementing the current standard with an additional inquiry into what information an individual disclosed when initiating a transaction. This modified standard would preserve the integrity of Bitcoin, while simultaneously articulating a proper framework for assessing privacy concerns in the context of Bitcoin and blockchain technology.*

# I. INTRODUCTION

Privacy has been central to Bitcoin since its inception.[1] Bitcoin was expressly created as a peer-to-peer form of digital cash, retaining privacy through the anonymity of public keys.[2] Bitcoin's key features of decentralization, distribution, and anonymity seem to reflect the original intent of the Fourth Amendment: preventing abuse by law enforcement.[3] Bitcoin grants privacy to its users, manifesting the Fourth Amendment ideals of security and autonomy in a digital world seemingly devoid of privacy.[4]

However, the creation of centralized exchanges, which act as financial institutions, and the government's ability to use commercial services to track transactions threaten the integrity of Bitcoin's blockchain technology.[5] As a result, it is no surprise that Bitcoin presents novel Fourth Amendment challenges for courts to consider.[6] Such challenges are especially significant considering the Supreme Court's repeated warnings against the ill suitability of Fourth Amendment jurisprudence in addressing privacy concerns arising out of technological advancements.[7] As Bitcoin and

1 *See* Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 6 (2008) (unpublished manuscript), https://bitcoin.org/bitcoin.pdf [https://perma.cc/M4V8-YDVL].

2 *See id*. at 1, 6 (describing how a peer-to-peer network eliminates the need for trusted third parties and retains privacy "by keeping public keys anonymous").

3 *See, e.g.*, Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1194 (2016); Matthew C. Woessner & Barbara Sims, *Technological Innovation and the Application of the Fourth Amendment: Considering the Implications of* Kyllo v. United States *for Law Enforcement and Counterterrorism*, 19 J. CONTEMP. CRIM. JUST. 224, 225 (2003).

4 *See* Nakamoto, *supra* note 1, at 6 (retaining privacy for its users by keeping private keys—and thus the identities of its users—anonymous). *See generally* Paul Belonick, *Transparency Is the New Privacy: Blockchain's Challenge for the Fourth Amendment*, 23 STAN. TECH. L. REV. 114, 134–36 (2020) (discussing the privacy Bitcoin grants to users).

5 *See* discussion *infra* Section II.C.

6 *See* Belonick, *supra* note 4, at 118.

7 *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (arguing that the Fourth Amendment's third-party doctrine "is

blockchain technology continue to increase in popularity,[8] it is important to consider how courts might apply Fourth Amendment doctrine when addressing privacy issues related to such technology.

In 1967, the Supreme Court altered the public/private distinction underlying Fourth Amendment doctrine: What is done in public could now be considered private.[9] This landmark decision limited the government's ability to encroach on an individual's privacy. However, the pendulum quickly swung the other way. In 1970, Congress enacted the Bank Secrecy Act,[10] which requires financial institutions to maintain and, if need be, share their clients' personal information with the government to assist in its investigations.[11] Soon after, the Supreme Court established the third-party doctrine, finding that information voluntarily handed over to a third party (e.g., a bank) is not protected by the Fourth Amendment.[12] Today, courts tend to decide whether an individual has a privacy interest by applying the

ill suited to the digital age"); *id.* at 427–30 (Alito, J., concurring) (advocating for legislative action); Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (limiting the applicability of the third-party doctrine); *id.* at 2262 (Gorsuch, J., dissenting) (discussing the interaction between technology and the Fourth Amendment).

8 The number of Bitcoin users has increased by 16 million from December 2020 to January 2021. Moreover, more than $14 billion worth of Bitcoin transactions occur each day and Bitcoin maintains close to 300,000 transaction every month. James Anthony, *Number of Blockchain Wallet Users 2022/2023: Breakdowns, Timelines, and Predictions*, FINS. ONLINE, https://financesonline.com/number-of-blockchain-wallet-users/ [https://perma.cc/A6MH-WUM3] (last visited May. 10, 2022).

9 *See* Katz v. United States, 389 U.S. 347, 351 (1967) (finding that placing an eavesdropping device on a public telephone booth constituted a search under the Fourth Amendment and that what an individual "seeks to preserve as private, even in area accessible to the public, may be constitutionally protected").

10 Pub. L. 91-508, 84 Stat. 1114 (1970).

11 12 U.S.C. § 1829b(a)(1) (2018).

12 *See* United States v. Miller, 425 U.S. 435 (1976) (finding no reasonable expectation of privacy in bank records); Smith v. Maryland, 442 U.S. 735 (1979) (finding no reasonable expectation of privacy in telephone call logs).

reasonable-expectation-of-privacy test, a subjective and objective test of perceived privacy.[13]

As noted, the Supreme Court has warned that Fourth Amendment jurisprudence is ill-equipped to deal with privacy issues related to emerging technologies. This growing concern led the Court to limit the applicability of the third-party doctrine in *Carpenter v. United States*.[14] However, it added the caveat that this decision "is a narrow one," leaving open the question of how, when, and to what extent the third-party doctrine applies to investigative tools.[15] Specifically, the Court left open the question of how to apply the third-party doctrine and the reasonable-expectation-of-privacy test to the Bitcoin blockchain.[16]

The Fifth Circuit tackled this question in *United States v. Gratkowski*, a case involving the purchase of child pornography using Bitcoin.[17] In a mere seven-page opinion, the court held that Gratkowski lacked a privacy interest in his personal information on both Coinbase, a centralized

[13] Justice Harlan, in his concurrence, understood the rule emerging "from prior decisions is 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.'" *Katz*, 389 U.S. at 361 (Harlan, J., concurring). The *Katz* Court established this "reasonable expectation of privacy" test that has been used in subsequent Fourth Amendment search and seizure litigation. *See Miller*, 425 U.S. at 440; *Smith*, 442 U.S. at 745; *Carpenter*, 138 S. Ct. at 2224 (finding a reasonable expectation of privacy in data acquired through cell-phone tracking technology, if held for more than six days). *But see* United States v. Jones, 565 U.S. 400 (2012) (applying the common-law-trespassory test, stating that it is not necessary to consider whether an individual has a reasonable expectation of privacy when there is physical instruction into a vehicle—an "effect" as written in the Fourth Amendment).

[14] *Carpenter,* 138 S. Ct. at 2208.

[15] *Id*. at 2220.

[16] *See* Belonick, *supra* note 4, at 114 (arguing that current Fourth Amendment doctrine rests "on physical-world analogies that do not hold in blockchain's unique digital space"); Lawrence J. Trautman, *Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace*, 102 MARQ. L. REV. 447 (2018) (describing the struggle for law and regulation to keep pace with emerging blockchain and cryptocurrency technology).

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

cryptocurrency exchange, and on the Bitcoin blockchain directly.[18] Notably, the court was the first to find that an individual does not have a reasonable expectation of privacy in their personal information stored directly on the blockchain.[19]

However, in reaching these findings, the Fifth Circuit applied inconsistent and flawed reasoning, demonstrating a fundamental misunderstanding of Bitcoin and its users.[20] The Fifth Circuit did not heed the Supreme Court's warning about the ill-suitability of Fourth Amendment doctrine in addressing privacy concerns arising out of technological advancements. Moreover, the Fifth Circuit went beyond the facts of the case to find that the defendant lacked a privacy interest in his information on the blockchain.

In negating Bitcoin's key features of decentralization and anonymity, *Gratkowski* may be devastating to the cryptocurrency and blockchain industries. The Fifth Circuit reasoned that Bitcoin users have no reasonable expectation of privacy in their transactions made directly on the Bitcoin blockchain, even though one of Bitcoin's most attractive features is the privacy it grants users. Thus, under *Gratkowski*, Bitcoin transactions are not afforded Fourth Amendment protection.[21] The Fifth Circuit's finding that users do not have a reasonable expectation of privacy when they transact in bitcoin, regardless of the digital wallet they use, completely nullifies Bitcoin's key features of anonymity and decentralization. Such a finding risks hindering the advancements and advantages of blockchain technology.

This Note argues that *Gratkowski* should be interpreted narrowly and with caution due to its flawed reasoning and potential ramifications for the blockchain industry. Part II discusses Bitcoin's key features, digital wallets, and cryptocurrency exchanges. Part III explains the evolution of Fourth Amendment jurisprudence, focusing on the Supreme

[18] *Id.* at 312–13. For background on the Bitcoin blockchain and Coinbase, see *infra* Part I.

[19] *Gratkowski*, 964 F.3d at 307.

[20] *See infra* Section IV.C.

[21] *See id.*; *Gratkowski*, 964 F.3d 307 at 312, 313.

Court case law used to justify the *Gratkowski* decision. Part IV discusses the *Gratkowski* opinion in detail and argues that the Fifth Circuit's reasoning is flawed. Finally, Part V makes the case for a narrow reading of *Gratkowski* and suggests supplementing the reasonable-expectation-of-privacy standard with an inquiry into what information an individual disclosed, if any, upon registration or installation of a digital wallet.

Under the suggested structure, the reasonable-expectation-of-privacy standard would remain. However, it is necessary to articulate a proper framework for applying that standard in the context of Bitcoin transactions. Not all Bitcoin transactions are the same, and not all Bitcoin users utilize the same methods of transacting.[22] Claiming otherwise would be a gross misunderstanding of the cryptocurrency market.[23] Contrary to the Fifth Circuit's over-simplification of all cryptocurrencies as essentially the same, different cryptocurrency wallets require varying types of personal disclosures upon installation and registration that implicate different levels of privacy concerns.[24] Asking what information an individual disclosed when registering may assist courts in reaching a fair and accurate decision regarding an individual's expectation of privacy when transacting in Bitcoin. An individual's expectation of privacy would thus depend on the digital wallet they used to transact and, therefore, what identifying information they gave up in order to register. This solution puts privacy back in the hands of individuals, while simultaneously preserving the integrity of Bitcoin and the Fourth Amendment ideals of ownership, security, and control.

22 *See* discussion *infra* Section II.B.

23 This is exactly what the Fifth Circuit did in its *Gratkowski* decision. *See infra* Section IV.C.

24 *See, e.g.*, *supra* Section II.B (comparing types of digital wallets).

## II. THE BITCOIN BLOCKCHAIN AND THE SIGNIFICANCE OF PRIVACY

Blockchain is an immutable, distributed ledger that allows users to timestamp, record, and track transactions.[25] Blockchain technology is used for cryptocurrencies—digital cash secured by cryptography.[26] The Bitcoin blockchain, for example, is a public ledger on which all Bitcoin transactions are recorded.[27] Since blockchain was conceived alongside Bitcoin "to create and record bitcoin transactions, . . . blockchain is often confused with Bitcoin."[28] However, blockchain itself is not a currency. Instead, it is a tool used to maintain an unchangeable, decentralized transaction history.[29] This technology validates and timestamps each change in ownership through cryptography, thus creating a secured ledger of transaction history.[30] Indeed, blockchain technology allows users to retrace ownership and more readily identify the present owner of an asset.[31] The possibilities for its utilization are seemingly endless. Blockchain technology is

25 *See* Michael Nofer et al., *Blockchain*, 59 BUS. & INFO. SYS. ENG'G 183, 183–84 (2017) ("A blockchain consists of data sets which are composed of a chain of data packages (blocks) where a block comprises multiple transactions. The blockchain is extended by each additional block and hence represents a complete ledger of the transaction history.").

26 *See* Belonick, *supra* note 4, at 117, 125. As of publication, there are more than 18,000 cryptocurrencies in existence. *Today's Cryptocurrency Prices by Market Cap*, COINMARKETCAP, https://coinmarketcap.com/ [https://perma.cc/NA26-4A6L] (last visited May 10, 2022).

27 Securities and Exchange Commission, Self-Regulatory Organizations; Cboe BZX Exchange, Inc.; Notice of Filing of a Proposed Rule Change To List and Trade Shares of the VanEck Bitcoin Trust, Under BZX Rule 14.11(e)(4), Commodity-Based Trust Shares, Exchange Act Release No. 91,326, 86 Fed. Reg. 14,987, 14,988 (notice March 15, 2021).

28 Belonick, *supra* note 4, at 117–18.

29 *See* Nofer et al., *supra* note 25, at 183.

30 *Id*. at 183–84.

31 *Id*.

already being used for smart contracts,[32] health records,[33] and supply chain management.[34]

Bitcoin remains the most popular application of blockchain,[35] and its key features demonstrate Bitcoin's emphasis on privacy.[36] First, Bitcoin is *decentralized*: It is a peer-to-peer network that eliminates the need for a trusted third party, enhancing privacy by giving users the ability to transact remotely without disclosing any personal

[32] *See id.* at 185 ("Thus, blockchain technology allows to establish contracts using cryptography and to replace third parties (e.g., a notary) that have been necessary to establish trust in the past. Blockchain might disrupt the entire transaction process by automatically executing contracts in a cost-effective, transparent and secure manner."); *see also* Deborah Ginsberg, *The Building Blocks of Blockchain*, 20 N.C. J.L. & TECH. 471, 487 (2019) ("Meanwhile, blockchain is changing the way common legal transactions function. The Ethereum programming language, for example, is being used to create smart contracts. These contracts are designed to be launched and run automatically—the parties rely on the code to handle the transaction on its own" (citation and footnote omitted)).

[33] *See* Taavi Einaste, *Blockchain and Healthcare: the Estonian Experience*, NORTAL (Feb. 21, 2018), https://nortal.com/blog/blockchain-healthcare-estonia/ [https://perma.cc/L7JB-7JP2] (noting that Estonia became the first country to use blockchain technology for healthcare on a national scale).

[34] *See IBM Supply Chain Intelligence Suite: Food Trust*, IBM, https://www.ibm.com/products/food-trust [https://perma.cc/EVK6-C773] (last visited May 10, 2022) ("IBM Food Trust[] is a collaborative network of growers, processors, wholesalers, distributors, manufacturers, retailers, and others, enhancing visibility and accountability across the food supply chain" built on IBM blockchain). This list is by no means exhaustive of the current and potential uses of blockchain technology. For more examples, see Adam Hayes, *Blockchain Explained*, INVESTOPEDIA (Mar. 5, 2022), https://www.investopedia.com/terms/b/blockchain.asp [https://perma.cc/H5VK-MRS8].

[35] *See* Anthony, *supra* note 8.

[36] Indeed, the Bitcoin whitepaper contains an entire section dedicated to privacy. *See* Nakamoto, *supra* note 1, at 6; *see also Protect Your Privacy*, BITCOIN, https://bitcoin.org/en/protect-your-privacy [https://perma.cc/L72M-5LT4] (last visited May 10, 2022) (dedicating a page to help users protect their privacy with recommendations, such as using a new Bitcoin address for every new payment; making sure not to disclose Bitcoin addresses; and being careful with public spaces generally).

information to a financial institution.[37] Second, Bitcoin is *distributed* and *open*: No one central authority can control or alter any of the transaction details because they are verified by cryptographic means and recorded on a publicly-viewable blockchain.[38] Finally, Bitcoin is *anonymous*: Public keys, also known as Bitcoin addresses, are kept anonymous to retain privacy alongside its public disclosure protocol.[39]

This Part first describes Bitcoin's key features of decentralization, distribution/openness, and anonymity. Additionally, it explains the use of digital wallets and the privacy considerations in choosing a digital wallet to transact peer-to-peer. It then examines cryptocurrency exchanges, demonstrating how centralized exchanges run counter to Bitcoin's philosophy. Finally, it includes a brief discussion of Bitcoin's association with criminal activity.

## A. Bitcoin's Features of Decentralization, Distribution/Openness, and Anonymity

The rising need for decentralization has been attributed to the mistrust of financial institutions stemming from the 2008 financial crisis and the issues it revealed, such as the challenge of retracing ownership.[40] The Bitcoin whitepaper, published in 2008, was authored by an anonymous person under the pseudonym Satoshi Nakamoto.[41] The domain name "bitcoin.org" was registered and created that same year,[42] and Bitcoin's peer-to-peer computer network was launched in

37 *See* Nakamoto, *supra* note 1, at 1. Decentralization means users do not have to rely on a central authority to verify all transactions. *See id.*; Avishay Yanay, *Bitcoin—Money Decentralization (Understanding the Process)*, VPN MENTOR, https://www.vpnmentor.com/blog/bitcoin-money-decentralization/ [https://perma.cc/8PDW-85YG] (last visited May 10, 2022).

38 *See* Nakamoto, *supra* note 1, at 1; Belonick, *supra* note 4, at 129.

39 Nakamoto, *supra* note 1, at 6.

40 *See* Belonick, *supra* note 4, at 123; Nofer et al., *supra* note 25, at 183.

41 *See* Nakamoto, *supra* note 1.

42 *See Bitcoin.org*, WHOIS, https://www.whois.com/whois/bitcoin.org [https://perma.cc/GG62-F5VR] (last visited May 10, 2022).

early 2009.[43] Nakamoto begins the whitepaper by stating that internet commerce relies "almost exclusively on financial institutions serving as trusted third parties to process electronic payments."[44] However, this system which uses what Nakamoto refers to as the "trust based model" has inherent weaknesses such as an increase in transaction costs, the loss of the ability to make non-refundable payments for non-reversible services, and fraud.[45] This "trust based model" creates a need for more trust because "[w]ith the possibility of reversal, the need for trust spreads[,]" and "[m]erchants must be wary of their customers, hassling them for more information than they would otherwise need."[46] As a result, people are giving out more information about themselves, giving up their privacy to conform to the current system.[47]

Nakamoto further states that although such "costs and payment uncertainties can be avoided in person by using physical currency, no mechanism exists to make payments over a communications channel without a trusted third party."[48] This is where Bitcoin comes in, a peer-to-peer form of digital cash that allows parties to transact directly with one

43 Paulina Likos & Coryanne Hicks, *The History of Bictoin, the First Cryptocurrency*, U.S. NEWS (Feb. 4, 2022, 12:57 PM), https://money.usnews.com/investing/articles/the-history-of-bitcoin (on file with the Columbia Business Law Review).

44 Nakamoto, *supra* note 1, at 1.

45 *Id*. ("Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable."); *see also* Nofer et al., *supra* note 25, at 183 ("Intermediaries perform the careful checking of each involved party along a chain of intermediaries. However, this is not only time consuming and costly but also bears a credit risk in case an intermediary fails.").

46 Nakamoto, *supra* note 1, at 1.

47 *See id*; *see also* Belonick, *supra* note 4, at 123.

48 Nakamoto, *supra* note 1, at 1.

another—that is, without a financial institution.[49] However, without a financial institution, there is no trusted third-party to process digital payments and protect the parties involved in a given transaction.[50] As it is, by its nature, decentralized, Bitcoin must remedy this issue.[51] Bitcoin's solution to these issues is grounding its electronic payment system in cryptographic proof.[52] Relying on math and technology rather than financial institutions remedies the issues of the trust-based model, protecting buyers and sellers from fraud, eliminating mediation costs, and increasing efficiency with instant payments.[53]

Bitcoins are transferred peer-to-peer, directly from buyer to seller.[54] As each digital coin is defined as a series of digital signatures, a "payee"—the party receiving bitcoin—uses the digital signatures to verify the chain of ownership and legitimacy of a bitcoin.[55] These signatures contain a timestamp, a hash value of the previous block, and the public key of the next owner (the payee).[56] A hash value is a string of random numbers and letters; it is unique and prevents fraud since any change would alter the hash value.[57]

---

[49] *Id.*

[50] *See id.* at 1–2, 6.

[51] Using trusted third parties, the traditional banking method limits access to information to the parties involved. As Bitcoin is decentralized—it does not rely on a trusted third party—it must break the flow of information elsewhere. Otherwise, the Bitcoin's public disclosure of all transactions would provide the information of every party involved. *Id.* at 2, 6.

[52] *Id.* at 1.

[53] *Id.* ("Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.").

[54] Nakamoto, *supra* note 1, at 1.

[55] *Id.* at 2, 8.

[56] *Id.* at 2, 7; Nofer et al., *supra* note 25, at 184.

[57] Nofer et al., *supra* note 25, at 184.

> A cryptographic "hash" algorithm is a mathematical formula that can convert any amount of data or text into a set length string of seemingly random characters. This conversion is called "hashing." The resulting string is called a "digest."

However, the payee also needs to verify that the bitcoin they are receiving has not already been spent (double-spending).[58] This is where Bitcoin's key distribution feature comes in: to eliminate the issue of double-spending without relying on a trusted third party, all Bitcoin transactions must be publicly announced.[59] The only way to confirm that digital cash has not already been expended without a trusted third party "is to be aware of all transactions."[60] The distributed and transparent nature of Bitcoin prevents double-spending and, thus, preserves trust between transacting parties.[61]

In this digital payment system based on cryptographic proof instead of trust, individuals who would otherwise give up information to conform to the trust-based model can retain their privacy and transact with one another without the need for a trusted third-party.[62] But the question then becomes: If all Bitcoin transactions are publicly announced, how do users retain privacy?[63] Bitcoin uses a cryptographic key system in which each user needs two keys for each transaction: "[t]he public key, also known as the Bitcoin address, is used to send and accept payments to and from other users, while the private key remains concealed with the user and functions as

> The genius of hashing is that the tiniest change to the input data generates a wildly different digest, with no apparent relation to the input data or to any other close variant.

Belonick, *supra* note 4, at 125 (footnotes omitted).

58 Nakamoto, *supra* note 1, at 2.

59 *Id*.

60 *Id*. ("We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions.").

61 *See* Nofer et al., *supra* note 25, at 184 ("Using cryptography, people all over the world can trust each other and transfer different kinds of assets peer-to-peer over the internet. . . . [Bitcoin's distributed ledger] increases trust since people do not have to assess the trustworthiness of the intermediary or other participants in the network.").

62 *Id*; *see also* Nakamoto, *supra* note 1, at 6.

63 *See* Nakamoto, *supra* note 1, at 6.

a password to unlock the transaction."[64] Moreover, the public key is kept anonymous so that it cannot be used to identify the user.[65] Anyone viewing the Bitcoin blockchain "can see that someone is sending an amount to someone else, but without information linking the transaction to anyone."[66] Nakamoto also recommends using new keys for each new transaction to keep transactions "from being linked to a common owner."[67] Bitcoin's public disclosure protocol—that all transactions are publicly announced—allows the features of decentralization, transparency, and anonymity to merge to innovate the way in which people transact.[68]

## B. Digital Wallets and Privacy Considerations

A digital wallet is a software that stores and tracks transactions.[69] When choosing a wallet, Bitcoin's website first asks users to select an operating system, giving the options of mobile wallets, desktop wallets, and hardware wallets.[70] Each choice describes the benefits and drawbacks of the particular

64 Jonathan Lane, *Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation*, 8 CHARLESTON L. REV. 511, 516 (2014) (footnotes omitted) ("The software generates two mathematically related keys, one public and one private, that together make up a user's digital signature. . . . For each public key, or Bitcoin address, there is exactly one matching private key that is mathematically related to it and is designed in a way that the public key may be calculated from it, but not vice-versa." (footnotes omitted)).

65 Nakamoto, *supra* note 1, at 6. Bitcoin's "system uses *two* keys: a *public* key that can be shared with others with whom one wishes to interact, and a secret *private* key known only to an individual user. . . . [T]he public key scrambles data, while only the private key can unscramble the data." Belonick, *supra* note 4, at 126 (footnotes omitted).

66 Nakamoto, *supra* note 1, at 6.

67 *Id*.

68 *See id*. at 2.

69 *See* Belonick, *supra* note 4, at 127 ("A common storage method is the so-called 'wallet,' a commercially-available software program that can store public and private keys and keep track of blockchain transactions.").

70 *Choose Your Bitcoin Wallet*, BITCOIN, https://bitcoin.org/en/choose-your-wallet?step=1 [https://perma.cc/3P9L-B3HP] (last visited May 10, 2022).

wallet, with the hardware wallet being "one of the most secure methods to store funds" because it stores a user's data offline.[71] Many desktop and mobile wallets improve privacy by not disclosing any information to peers on the network and using Tor[72] as a proxy to prevent the association of payments with IP addresses.[73]

Wallets that are connected to the internet are referred to as "hot wallets," while hardware wallets—wallets that are disconnected from the internet—use the "cold storage method."[74] The cold storage method is a more secure means of storing cryptocurrency, as hot wallets are vulnerable to hacking.[75] Some hot wallets, such as Mycelium, offer the added feature of cold storage integration—allowing users to store data offline on a hardware wallet.[76]

Once a new user has a wallet installed, they receive their first Bitcoin address (i.e., public key), which they can disclose

71 *Id*.

72 Tor, or onion routing, is a means of browsing the web anonymously by routing internet traffic through multiple servers, scrambling data so that the original IP address cannot be traced. *See About: History*, TOR PROJECT, https://www.torproject.org/about/history/ [https://perma.cc/Z4Z2-YBF9] (last visited May 10, 2022). For more information on Tor, see Jake Frankenfield, *Tor Definition*, INVESTOPEDIA (Feb. 13, 2022), https://www.investopedia.com/terms/t/tor.asp [https://perma.cc/PJR2-K3NH].

73 Bitcoin Core is one such wallet provider. *See Bitcoin Core*, BITCOIN, https://bitcoin.org/en/wallets/desktop/mac/bitcoincore/?step=5&platform=mac [https://perma.cc/53U8-5J5L] (last visited May 10, 2022) ("Bitcoin Core is a full Bitcoin client and builds the backbone of the network. It offers high levels of security, privacy, and stability.").

74 Jake Frankenfield, *Hot Wallet*, INVESTOPEDIA (Jan. 8, 2022), https://www.investopedia.com/terms/h/hot-wallet.asp [https://perma.cc/W2LT-8JXT].

75 *Id*.

76 *Id*.; *see* Luke Conway, *Best Bitcoin Wallets*, INVESTOPEDIA (May 4, 2022), https://www.investopedia.com/best-bitcoin-wallets-5070283 [https://perma.cc/368T-W2JW] (deeming Mycelium to be the best Bitcoin wallet for mobile users "because it gives [users] more control over transaction fees and integrates with a hardware wallet," meaning it "allow[s] users to hold their Bitcoin in an offline storage device while still using Mycelium's user interface to see their holdings.").

to receive payment.[77] A different Bitcoin address is used for each new transaction to avoid associating several transactions with a common owner.[78] Once a payee receives the encrypted public key, a private key is used to decrypt the data and place the electronic cash into the payee's own wallet.[79]

The facts of *United States v. Costanzo*, an appeal of a money laundering conviction involving the transfer of bitcoin, exemplify the use of digital wallets.[80] During the course of an undercover investigation into Costanzo, an undercover agent "explicitly told Costanzo that he was trafficking black tar heroin" and requested to exchange $3,000 in cash for bitcoin.[81] The two made a transaction using Mycelium wallet, a digital wallet which does not require identification of any kind.[82] When making a transaction using a mobile wallet, a "QR code is used to scan the public address needed to transfer bitcoin from the digital wallet on one phone to the digital wallet on another phone, and the recipient can then access the bitcoin using a private key."[83] Costanzo and undercover agents continued to communicate through encrypted messages, and during their subsequent meetings, "the undercover agents made clear to Costanzo that the purpose of the transaction was to conceal illegal activities."[84] The Ninth Circuit ultimately affirmed Costanzo's money laundering conviction because it held that the bitcoin transfers had the necessary effect on interstate commerce.[85]

---

77 *How Does Bitcoin Work?*, BITCOIN, https://bitcoin.org/en/how-it-works [https://perma.cc/SHV2-BGPU] (last visited May 10, 2022).

78 Nakamoto, *supra* note 1, at 6.

79 *See* Belonick, *supra* note 4, at 128.

80 United States v. Costanzo, 956 F.3d 1088, 1093 (9th Cir. 2020) (holding that there was sufficient evidence to support the finding that the money laundering transactions in question affect interstate commerce).

81 *Id*. at 1090.

82 MYCELIUM, https://wallet.mycelium.com/#home [https://perma.cc/HA4D-PZUW] (last visited May 10, 2022); *see supra* note 76.

83 *Costanzo,* 956 F.3d at 1091.

84 *Id*. at 1090.

85 *Id*. at 1092 (finding that the government presented sufficient evidence "to prove that Costanzo 'conduct[ed] or attempt[ed] to conduct a

## C. Exchanges and Privacy Considerations

Bitcoin users also have the option to transact using centralized or decentralized cryptocurrency exchanges.[86] Centralized cryptocurrency exchanges are for-profit private companies that provide cryptocurrency trading services.[87] They are centralized because they are controlled by a single entity—a private company utilizing private servers to facilitate the exchange of digital assets.[88] Moreover, centralized exchanges must require their users to disclose personal information, because they are subject to state and federal laws that impose obligations such as anti-money laundering laws and know-your-customer rules.[89] Thus, when

financial transaction" with the intent 'to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity'" (quoting 18 U.S.C. §§ 1956(a)(1), (a)(3)(B) (2018))). Notably, the fact that Costanzo transferred bitcoin through a digital wallet that required the internet, implicates an international network and interstate commerce, even though both parties were located in the same state. *See id.* For a definition of a "financial transaction," see 18 U.S.C. § 1956(c)(4).

86 Cryptocurrency exchanges facilitate the trading of cryptocurrencies for other cryptocurrencies or fiat money. Kristin N. Johnson, *Regulating Cryptocurrency Secondary Market Trading Platforms*, 2020 U. CHI. L. REV. ONLINE 26, 37.

87 *Id.* Coinbase, Kraken, and Binance are examples of well-known centralized exchanges, "which allow the purchase and sale of virtual currencies through fiat currency payments and are, therefore, the main points of access to the market for virtual assets." David Silva Ramalho & Nuno Igreja Matos, *What We Do in the (Digital) Shadows: Anti-Money Laundering Regulation and a Bitcoin-Mixing Criminal Problem*, 22 ERA F. 487, 499 (2021).

88 Johnson, *supra* note 86, at 37.

89 *Id.*

> As custodians of financial assets, centralized exchanges must comply with state and federal laws relevant to the custody, exchange, and transfer of assets including federal anti-money-laundering and know-your-customer user-verification obligations. Consequently, the Financial Crimes Enforcement Network ("FinCEN"), a bureau of the United States Department of the Treasury, may also regulate these cryptocurrency platforms as "money services business."

an individual opts for a centralized exchange such as Coinbase, they cannot retain anonymity or hide their identity from the company.[90] Still, centralized exchanges are among the most popular digital wallets because they are more convenient and much easier to use.[91]

Using a centralized cryptocurrency exchange has major drawbacks in terms of retaining privacy and anonymity.[92] Coinbase, one such centralized cryptocurrency exchange, is one of the most widely used digital wallets.[93] It is licensed as a "money services business,"[94] and money services businesses fall under the regulatory definition of "financial institutions" according to the U.S. Treasury.[95] However, Bitcoin was created to be a peer-to-peer form of digital cash, eliminating the reliance on financial institutions.[96] Thus, using a centralized exchange (e.g., Coinbase) completely negates the

*Id.*

90 *Id.*

91 *How To Set up a Crypto Wallet*, COINBASE, https://www.coinbase.com/learn/tips-and-tutorials/how-to-set-up-a-crypto-wallet [https://perma.cc/N7X4-MM36] (last visited May 10, 2022).

92 Coinbase requires its users to provide their personal information, completely negating the features of anonymity and privacy that Bitcoin and blockchain technology offer. *Coinbase User Agreement*, COINBASE, https://www.coinbase.com/legal/user_agreement/united_states [https://perma.cc/9ZRM-KCH3] (last updated May 10, 2022). Personal information Coinbase requires includes the "your name, address, telephone number, e-mail address, date of birth, taxpayer identification number, government identification, and information regarding your bank account (such as the name of the bank, the account type, routing number, and account number) and in some cases (where permitted by law), special categories of personal data, such as your biometric information". *Id.*

93 Raynor de Best, *Ranking of Cryptocurrency Wallet Apps in the U.S. 2017-2021*, STATISTA (Jan. 27, 2022), https://www.statista.com/statistics/1206619/most-popular-cryptocurrency-wallets-usa/ [https://perma.cc/MN34-CBDH].

94 31 C.F.R. § 1010.100(ff) (2021); *see Coinbase Money Transmission and e-Money Regulatory Compliance*, COINBASE, https://help.coinbase.com/en/coinbase/privacy-and-security/other/coinbase-regulatory-compliance (on file with the Columbia Business Law Review) (last visited May 10, 2022).

95 31 C.F.R. § 1010.100(t).

96 Nakamoto, *supra* note 1, at 1.

purpose of Bitcoin, as Coinbase users are still relying on a financial institution to store their digital cash. In fact, the Bitcoin website warns users that exchanges provide differing levels of safety and privacy.[97] Coinbase notifies users that it "reserve[s] the right at all times to monitor, review, retain and/or disclose any information as necessary to satisfy any applicable law, regulation, sanctions programs, legal process or governmental request."[98] Thus, when an individual opts for Coinbase as their means of transacting in bitcoin, they are sacrificing privacy for convenience.

Decentralized exchanges, on the other hand, do not rely on any central authority—or server—to store cryptocurrency.[99] They are peer-to-peer platforms, more in line with Bitcoin's philosophy, that match up traders to facilitate transactions.[100] Because no single entity retains control over a user's funds, no entity maintains identifying information of their users.[101] For example, Bisq, a decentralized cryptocurrency exchange, does not require any registration to download and use the service.[102] Thus, individuals may protect their identities and retain privacy when using a decentralized exchange.

---

[97] *Bitcoin Exchanges*, BITCOIN, https://bitcoin.org/en/exchanges [https://perma.cc/2DE9-CQEG] (last visited May 10, 2022).

[98] *Coinbase Global Privacy Policy*, COINBASE, https://www.coinbase.com/legal/privacy#why-we-share-personal-information-with-other-parties [https://perma.cc/T7UB-LJGX] (last updated May 10, 2022) (explaining that Coinbase shares personal information "[w]ith law enforcement, officials, or other third parties when [they] are compelled to do so by a subpoena, court order, or similar legal procedure, or when we believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity, or to investigate violations of [their] User Agreement or any other applicable policies").

[99] Johnson, *supra* note 86, at 38.

[100] *Id.*

[101] *Id.* ("Depending on the [decentralized exchange's] framework, the trader either maintains custody of their tokens at all times or gives up custody to the [decentralized exchange's] smart contract until a particular trade is executed and settled.").

[102] BISQ, https://bisq.network/ [https://perma.cc/CX2S-CHJU] (last visited May 10, 2022).

## D. Bitcoin and Criminality

Notably, Bitcoin's features of anonymity and decentralization attract criminal activity.[103] In the past, individuals have used Bitcoin and blockchain technology to facilitate illegal activities including, but not limited to, money laundering,[104] drug trafficking,[105] child exploitation,[106] assassination plots,[107] and sale of armaments.[108] However, such criminal activity does not detract from the benefits or

103 *See, e.g.*, Trautman, *supra* note 16, at 467–70 ("By 2013, Bitcoin had gained widespread notoriety as an anonymous vehicle for the transmission of funds involved in illegal activities." (citations and footnote omitted)); *see also* Mengqi Sun & David Smagalla, *Cryptocurrency-Based Crime Hit a Record $14 Billion in 2021*, WALL ST. J. (Jan. 6, 2022, 6:20 PM), https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073 (on file with the Columbia Business Law Review).

104 *See, e.g.*, United States v. Costanzo, 956 F.3d 1088 (9th Cir. 2020) (an appeal involving a conviction of five counts of money laundering, in which payment was made using Bitcoin).

105 *See* Trautman, *supra* note 16, at 467; U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-105462, VIRTUAL CURRENCIES: ADDITIONAL INFORMATION COULD IMPROVE FEDERAL AGENCY EFFORTS TO COUNTER HUMAN AND DRUG TRAFFICKING 1 (2021), https://www.gao.gov/assets/gao-22-105462.pdf [https://perma.cc/S6W7-8G2S].

106 *See, e.g.*, United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020) (involving a website that facilitated the purchase, sale, and distribution of child pornography).

107 *See, e.g.*, Sebastian Sinclar, *U.S. Woman Charged with Attempted Dark Web Murder-for-Hire Paid with Bitcoin*, COINDESK (Feb. 9, 2021, 4:58 AM), https://www.coindesk.com/policy/2021/02/09/us-woman-charged-with-attempted-dark-web-murder-for-hire-paid-with-bitcoin/ [https://perma.cc/MT2V-G377]; Andy Greenberg, *Meet The 'Assassination Market' Creator Who's Crowdfunding Murder with Bitcoins*, FORBES (Nov. 18, 2013, 8:30 AM), https://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/?sh=5b0d3e4a3d9b [https://perma.cc/3J3V-6J9W].

108 *See, e.g.*, Trautman, *supra* note 17, at 467–68, 467; Yessi Bello Perez, *U.S. Arms Dealer Allegedly Used Bitcoin for Purchases*, COINDESK (Aug. 12, 2015, 1:48 PM), https://www.coindesk.com/markets/2015/08/12/us-arms-dealer-allegedly-used-bitcoin-for-purchases/ [https://perma.cc/ZM6J-ZGE2].

legitimacy of blockchain technology, especially considering its relatively low prevalence as a share of all transactions. In 2021, "[t]ransactions involving illicit addresses represented just 0.15% of cryptocurrency transaction volume."[109] The stereotype that cryptocurrency is only for criminals is simply inaccurate.[110] Although criminal activity should always be a concern for law enforcement and regulatory bodies, it should not be a determining factor in a court's Fourth Amendment analysis. Rather, as this Note argues, courts should continue to apply the reasonable-expectation-of-privacy standard, supplemented with the additional inquiry into what information an individual gave up when opting for a digital wallet.[111]

## III. TECHNOLOGICAL ADVANCEMENTS AND THE FOURTH AMENDMENT

Technology has not only influenced the way people live their daily lives, but has also transformed the way law enforcement investigates and monitors criminal activity.[112] From the development of telephones to the use of GPS, emerging technology continuously presents new Fourth Amendment challenges for courts to consider.[113] This Part first discusses how the Supreme Court fundamentally altered the public/private distinction underlying Fourth Amendment

109 *Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity*, CHAINALYSIS (Jan. 6, 2022), https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/ [https://perma.cc/A479-DDCE].

110 Belonick, *supra* note 4, at 118 & n.22 (citing Wilma Woo, *U.S. DEA "Actually Wants" Criminals to Keep Using Bitcoin*, BITCOINIST (Aug. 8, 2019), https://bitcoinist.com/dea-wants-criminals-use-bitcoin [perma.cc/G4MC-ARAL] ("[T]he percentage of Bitcoin transactions tied to criminal activity had dropped from 90 percent in 2013 to just 10 percent in 2018.")).

111 *See* discussion *infra* Section V.B.

112 *See, e.g.*, United States v. Jones, 565 U.S. 400 (2021) (GPS tracking technology); Carpenter v. United States, 138 S. Ct. 2206 (2018) (cell-phone tracking technology).

113 *Id.*

doctrine by establishing the reasonable-expectation-of-privacy test and the third-party doctrine. It then looks at the Supreme Court's assertion that Fourth Amendment jurisprudence is ill-equipped to address technological advancements.

## A. The Public/Private Distinction: The Reasonable Expectation of Privacy and the Third-Party Doctrine

In order to thwart any future abuse by the country's new federal government,[114] the Fourth Amendment was ratified to protect "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[115] A search is per se unreasonable if it is "conducted outside the judicial process, without prior approval by [a] judge or magistrate."[116] A search occurs when the government (e.g., law enforcement) physically intrudes on a protected area "for the purpose of obtaining information."[117]

Technological advancements present an array of Fourth Amendment challenges for the judiciary to consider.[118] In some cases, the Court has avoided the issue at the nexus of technology and the constitutional right to privacy by using other interpretive methods to reach the same finding.[119] For example, in *Silverman v. United States*, law enforcement used a microphone to record conversations about the defendants'

114 Woessner & Sims, *supra* note 3, at 225.

115 U.S. CONST. amend. IV.

116 Mincey v. Arizona, 437 U.S. 385, 390 (1978) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)).

117 *Jones*, 565 U.S. at 404–05 (finding that a physical intrusion into an individual's vehicle constitutes a "search" under the Fourth Amendment).

118 *See, e.g.*, Woessner & Sims, *supra* note 3, at 224 (arguing "that the *Kyllo* standard for the application of sensory- enhancing technology has important implications for the future of law enforcement and the ongoing fight against international terrorism"); *see also* Trautman, *supra* note 17 (describing the struggle for law and regulation to keep pace with emerging blockchain and cryptocurrency technology).

119 *See, e.g.*, *Jones*, 565 U.S. at 404–05 (applying the common-law-trespassory test, stating that it is not necessary to consider whether an individual has a reasonable expectation of privacy when there is physical instruction into a vehicle—an "effect" as written in the Fourth Amendment).

gambling business.[120] Rather than addressing whether private conversations are generally constitutionally protected by the Fourth Amendment, the Court reasoned that "[e]avesdropping accomplished by means of such a physical intrusion" constitutes a search into a the constitutionally protected personal dwellings of the defendants.[121] But what if there was no physical intrusion? Basing a decision on the presence of a physical intrusion leaves open the question of what the Fourth Amendment protects, with or without physical intrusion.[122]

In *Katz v. United States*, the Supreme Court clarified that "what [an individual] seeks to preserve as private, even in area accessible to the public, may be constitutionally protected," fundamentally altering the public-private distinction in Fourth Amendment jurisprudence.[123] The majority found that the defendant, who entered a glass phonebooth to make a call, did not preclude his right to make a *private* call simply because he made the call in a seemingly *public* place—a place where he might be seen.[124] Justice Harlan, in his concurrence, understood the rule emerging "from prior decisions is 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.'"[125] The Supreme Court thus established this "reasonable expectation

120 Silverman v. United States, 365 U.S. 505 (1961).

121 *Id.* at 510. The Court later returned to this issue in *Wong Sun v. United States*, stating that "the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.'" 371 U.S. 471, 485 (1963). In *Katz*, the Court found that attaching an eavesdropping device to a public telephone booth constituted a search. Katz v. United States, 389 U.S. 34 (1967).

122 *See Jones*, 565 U.S. at 414, 417 (Sotomayor, J., concurring) (pointing out that that the majority opinion is too narrow in scope to address technological advancements in surveillance); *id.* at 419 (Alito, J., concurring) (emphasizing the inadequacies of the common-law-trespassory test).

123 *Katz*, 389 U.S. at 351.

124 *Id.*

125 *Id.* at 361 (Harlan, J., concurring).

of privacy" test that would be used in subsequent Fourth Amendment search and seizure litigation.[126] The *Katz* decision extended the scope of Fourth Amendment protections to include, in some cases, public places.[127]

Soon after, the third-party principle was adopted by the Supreme Court in two cases that both found that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party."[128] In *United States v. Miller*, the Court addressed whether an individual has a Fourth Amendment interest in their bank records.[129] The Court answered no, finding that

> [t]he lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they "have a high degree of usefulness in criminal tax, and regulatory investigations and proceedings."[130]

In *Smith v. Maryland*, the Court narrowed the scope of Fourth Amendment protections, clarifying its earlier

---

[126] *Id.*; *see, e.g.*, *Jones*, 565 U.S. at 401 ("[T]he *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test." (emphasis omitted)).

[127] *Katz*, 389 U.S. at 351. Several months after the *Katz* decision, the Court found that wiretapping constitutes a Fourth Amendment search and seizure and deemed unconstitutional a New York statute that authorized wiretapping without procedural safeguards. Berger v. New York, 388 U.S. 41 (1967); *see also* Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189, 192 (1996) ("Soon after *Katz*, in *Berger v. New York*, the Court reiterated that monitoring a conversation electronically is a search and seizure of words under the Fourth Amendment, and enumerated the requirements a statute must meet in order to constitutionally authorize wiretaps." (footnotes omitted)).

[128] United States v. Miller, 425 U.S. 435, 443 (1976); *accord* Smith v. Maryland, 442 U.S. 735, 744 (1979); *see also* Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963); United States v. White, 401 U.S. 745, 752 (1971).

[129] *Miller*, 425 U.S. at 436–37.

[130] *Id.* at 442–43 (citing 12 U.S.C. § 1829b(a)(1)).

decisions by stating that "a person has no legitimate expectation of privacy in information [they] voluntarily turn over to third parties."[131] The *Smith* Court addressed whether an individual has a privacy interest in their telephone call logs.[132] In answering no, the Court found that an individual does not have a subjective expectation of privacy in the numbers they dial, and, even if they did, this expectation would not be "legitimate" (i.e., not one that society would find reasonable).[133]

## B. The Unsuitability of Fourth Amendment Jurisprudence in Addressing Technological Advancements

In 2012, the Supreme Court again considered a case looking at the interplay of technological advancement and the Fourth Amendment.[134] In *United States v. Jones*, the Court addressed whether the use of GPS tracking technology in monitoring a vehicle's movements constitutes a search under the meaning of the Fourth Amendment.[135] Justice Scalia,

131 *Smith*, 442 U.S. at 743–44.

132 *Id.* at 736 ("This case presents the question whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment, made applicable to the States through the Fourteenth Amendment." (internal citations and footnotes omitted)).

133 *Id.* at 745 ("We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.'"). Justice Stewart dissented and argued that, like the Court found in *Katz*, an individual making a call in the privacy of their home is entitled to their reasonable expectation that that the contents of the call will be kept private. *Id.* at 752 (Stewart, J., dissenting) ("Just as one who enters a public telephone booth is 'entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,' so too, he should be entitled to assume that the numbers he dials in the privacy of his home will be recorded, if at all, solely for the phone company's business purposes." (quoting Katz v. United States, 389 U.S. 347, 352 (1967))).

134 *See* United States v. Jones, 565 U.S. 400, 400, 409 (2012) (holding that using GPS tracking technology to monitor a vehicle's movements constitutes a search and seizure).

135 *Id.* at 402 ("We decide whether the attachment of a Global–Positioning–System (GPS) tracking device to an individual's vehicle, and

writing for the majority, found no need to apply the reasonable-expectation-of-privacy test.[136] This is because a vehicle falls under the category of "effects" as written in the Fourth Amendment and, as such, a physical intrusion into a person's vehicle constitutes a common law trespass.[137] Justice Scalia emphasized that the reasonable-expectation-of-privacy test augments the common law trespass test for determining whether some government action constitutes a search; however, it does not completely replace it.[138]

The two concurring opinions in *Jones* discussed the inadequacies in the majority opinion.[139] Justice Sotomayor noted that the majority opinion is too narrow in scope to address technological advancements in surveillance.[140] Justice Alito, along with three other justices, advocated for applying the reasonable-expectation-of-privacy test, warning that the majority holding "strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial."[141] Justice Alito also pointed out that Justice Scalia employed reasoning very similar to that found in *Silverman*.[142] Rather than addressing whether conversations are constitutionally

subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment.").

136 *Id.* at 406.

137 *Id.* at 401. ("Here, the Government's physical intrusion on an 'effect' for the purpose of obtaining information constitutes a 'search.' This type of encroachment on an area enumerated in the Amendment would have been considered a search within the meaning of the Amendment at the time it was adopted.")

138 *Id.* at 409 ("But as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test.").

139 *See id.*

140 United States v. Jones, 565 U.S. 400, 414, 417 (2012) (Sotomayor, J., concurring).

141 *Id.* at 419 (Alito, J., concurring) ("I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.").

142 *Id.* at 421 (Alito, J., concurring).

protected by the Fourth Amendment, the *Silverman* Court reasoned that "[e]avesdropping accomplished by means of a physical intrusion" constituted a search into the constitutionally protected personal dwellings of the defendants.[143] Discussing the criticism and aftermath of *Silverman*, Justice Alito stressed the inadequacy of the common-law-trespassory test.[144] Applying the reasonable-expectation-of-privacy test, Justice Alito found that long-term tracking of a vehicle's location constitutes a search.[145]

In their respective concurrences, Justice Sotomayor and Justice Alito stressed the ill-suitability of Fourth Amendment doctrine in addressing privacy concerns arising from technological advancements.[146] Justice Sotomayor discussed the incompatibility of the third-party doctrine with the digital age, explicitly stating that "fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[147] Justice Alito advocated for

143 Silverman v. United States, 365 U.S. at 509, 512 (1961); *see Jones*, 565 U.S. at 421 (Alito, J., concurring) ("By contrast, in cases in which there was no trespass, it was held that there was no search."); *see also* Olmstead v. United States, 277 U.S. 438 (1928) (finding that the wiretapping of telephones did constitute a Fourth Amendment violation as there was no physical intrusion or seizure of defendants' effects), *overruled* by Katz v. United States, 389 U.S. 347 (1967); Goldman v. United States, 316 U.S. 129 (1942) (finding that the evidence obtained through the installation of a listening device did not violate the Fourth Amendment), *overruled* by *Katz*, 389 U.S. 347.

144 *Jones*, 565 U.S. at 423 (Alito, J., concurring) ("Under this approach, as the Court later put it when addressing the relevance of a technical trespass, 'an actual trespass is neither necessary *nor sufficient* to establish a constitutional violation.'" (emphasis added) (citing United States v. Karo, 468 U.S. 705, 713 (1984))).

145 *Id.* at 431 (Alito, J., concurring).

146 *Id.* at 417 (Sotomayor, J., concurring); *id.* at 427 (Alito, J., concurring).

147 *Id.* at 417 (Sotomayor, J., concurring). Sotomayor argued,

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their

legislative action, stating that "concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions" and that the legislative body is best-suited to address concerns at the crux of technology and privacy.[148]

In 2018, the Supreme Court addressed the issue of whether an individual has a reasonable expectation of privacy in the record of their physical movements as captured through cell-phone tracking technology (CSLI).[149] CSLI implicates both the third-party doctrine as well as the tracking of physical movement over time[150]—the same issue addressed in *Jones*.[151] Although the data at issue was voluntarily disclosed to a third party, the Court declined to extend *Miller* and *Smith* to CSLI.[152] Cell-phone tracking is unique in that it gives "the Government near perfect surveillance and allow[s] it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers."[153] Thus, *Carpenter* limited the applicability of the third-party doctrine in Fourth Amendment jurisprudence.[154]

However, the Court added a caveat to its *Carpenter* opinion: The decision is to be read narrowly.[155] The majority stated that the decision does "not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security

> cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailersI would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

*Id.* at 417–418.

148 *Id.* at 427–30 (Alito, J., concurring).

149 Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

150 *Id.* at 2263.

151 *Jones,* 565 U.S. 402.

152 *Carpenter*, 138 S. Ct. at 2217.

153 *Id.* at 2210.

154 *See id.*

155 *Id. at* 2220.

cameras."[156] This stipulation left open the question of what surveillance tools and techniques are considered "conventional" and how *Carpenter* should be applied in future cases involving innovative and disruptive technologies. These questions directly implicate Bitcoin and blockchain technology because government agencies employ commercial services to track and monitor transactions.[157] Moreover, Bitcoin's features of decentralization, transparency, and anonymity are challenged by the creation of third-party exchanges which deem themselves financial institutions (e.g., Coinbase).[158] It is, therefore, clear why Fourth Amendment jurisprudence is at the forefront of Blockchain and Bitcoin litigation.[159]

## IV. THE *GRATKOWSKI* DECISION

In a recent case looking at the interplay of cryptocurrency and Fourth Amendment privacy rights, the Fifth Circuit addressed the novel issue of "whether an individual has a Fourth Amendment privacy interest in the records of their Bitcoin transactions."[160] The court held that (1) the defendant lacked a privacy interest in his personal information located on Coinbase,[161] and (2) the defendant lacked a privacy interest in his information located directly on the blockchain.[162]

This Part first summarizes the facts of *Gratkowski*. It then explores the Fifth Circuit's finding that Gratkowski lacked a

156 *Id*.

157 Will Yakowicz, *Startups Helping the FBI Catch Bitcoin Criminals,* INC. (Jan. 9, 2018), https://www.inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html (on file with the Columbia Business Law Review).

158 *See supra* Section II.C.

159 *See* Belonick, *supra* note 4, at 118.

160 United States v. Gratkowski, 964 F.3d 307, 310 (5th Cir. 2020).

161 *Id*. at 313. As noted, Coinbase is a centralized exchange that stores users' digital cash. *Supra* notes 93–98 and accompanying text.

162 *Gratkowski*, 964 F.3d at 312. Blockchain is an immutable, distributed ledger that allows users to timestamp, record, and track transactions.

privacy interest in his Coinbase records, arguing that the court was justified in this holding. Finally, it examines the Fifth Circuit's finding that Gratkowski lacked a privacy interest in his personal information on the blockchain, pointing out the flaws and inconsistencies that highlight the court's misunderstanding of Bitcoin and its users.

## A. Facts of *United States v. Gratkowski*

In 2016, federal agents began an investigation into a child pornography website ("the Website").[163] Federal agents could not find the Website server's location using conventional investigation methods, such as IP address lookups. [164] This is because it was a Tor-based website,[165] "meaning it anonymize[s] Internet activity by routing user's communication through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ('IP') address of the user." [166] During the course of the investigation, federal agents discovered that some users were paying the site in bitcoin to download material.[167] After setting up an account on the Website and paying for premium access, the federal agents learned that the Website would provide each customer an address—a public key—to which to send bitcoin payments.[168]

Bitcoin transactions are publicly announced, but the identities of the transacting parties remain anonymous.[169] However, the federal agents had a remedy: using a commercial service to analyze the blockchain and identify

163 Brief of Appellee at 4, United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020) (No. 19-50492).

164 *Id.*

165 *Id.*

166 United States v. Galarza, No. 18-mj-146 (RMM), 2019 WL 2028710, at *2 (D.D.C. May 8, 2019) (internal quotation marks omitted) (quotation omitted); *see also supra* note 72.

167 *Gratkowski*, 964 F.3d at 309.

168 Brief of Defendant-Appellant at 6, United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020) (No. 19-50492).

169 *See supra* notes 64–66 and accompanying text.

"clusters" of Bitcoin addresses.[170] These investigative services analyze the blockchain by identifying patterns or clusters of associated Bitcoin addresses and then tracking that money back to an exchange or bank account.[171] Law enforcement agencies are increasingly using these tools to combat criminal activity funded via Bitcoin, so much so that CipherTrace, a blockchain analytics service, receives more than half of its California-based revenue from law enforcement agencies.[172]

The federal agents used one of these commercial services, analyzed the Bitcoin blockchain, and identified the site's Bitcoin addresses.[173] The agents then subpoenaed Coinbase for all information on the users who had sent bitcoin to the site's addresses.[174] Coinbase provided the information and identified Gratkowski as having used bitcoin to pay the child pornography site on six separate occasions.[175] The information Coinbase provided led to a search warrant for Gratkowski's house.[176] During the search, federal agents found a hard drive containing 190 images of child pornography in his home; Gratkowski then confessed and was arrested.[177]

Moving to suppress the evidence obtained through the search warrant, Gratkowski argued that the subpoena to Coinbase and the blockchain analysis violated his Fourth

170 Brief of Appellee, *supra* note 164, at 2–3.

171 Yakowicz, *supra* note 157.

172 *Id.* CipherTrace is funded by the Department of Homeland Security. *About Us*, CIPHERTRACE, https://ciphertrace.com/about-us/ [https://perma.cc/AW5Z-ZLNS] (last visited May 10, 2022).

173 Brief of Defendant-Appellant, *supra* note 180, at 7; Yakowicz, *supra* note 157.

174 Yakowicz, *supra* note 157.

175 Brief of Appellee, *supra* note 163, at 3.

176 *Gratkowski*, 964 F.3d 307 at 309.

177 *Id.*; Brief of Appellee, *supra* note 163, at 3.

Amendment right to privacy.[178] The district court denied the motion and Gratkowski appealed.[179]

The Fifth Circuit addressed this "novel question of whether an individual has a Fourth Amendment privacy interest in the records of their Bitcoin transactions."[180] Specifically, the court addressed (1) whether Gratkowski had a reasonable expectation of privacy in his information on the blockchain and (2) whether Gratkowski had a reasonable expectation of privacy in his information on Coinbase.[181] The court answered no to both of these questions.[182]

## B. *Grakowski*: Applying the Third-Party Principle to Coinbase

As noted, while the Supreme Court limited the applicability of the third-party doctrine in *Carpenter*, the Court warned that the decision should be read narrowly and left open the question of which circumstances fall under the scope of *Miller* and *Smith*.[183] The Fifth Circuit tried its hand at answering this question as it pertains to Coinbase, becoming the first federal appellate court to address this matter.[184]

The Fifth Circuit correctly found that the third-party doctrine applies to Coinbase records.[185] Gratkowski argued

178 *Gratkowski*, 964 F.3d at 310 ("Under the third-party doctrine, a person generally 'has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'" (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979))). Relying on *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018), which limited the applicability of the third-party doctrine in the context of cell phones, Gratkowski argued that the government violated his reasonable expectation of privacy in the records of his Bitcoin transactions on (1) Bitcoin's public blockchain and (2) Coinbase. In that regard, Gratkowski argued "that the district court erred in denying his suppression motion." *Gratkowski*, 964 F.3d at 310.

179 *Gratkowski*, 964 F.3d at 310.

180 *Id.* at 311–13.

181 *Id.* at 312–13.

182 *Id.*

183 *See supra* Section III.B.

184 *Gratkowski*, 964 F.3d 307 at 310 n.3.

185 *See id.* at 312.

that *Carpenter*'s limitation of the third-party doctrine should extend to Bitcoin transactions, and that the court should thus find that he has a privacy interest—that is, a reasonable expectation of privacy—in his Coinbase records.[186] However, the court rejected this argument and found that Coinbase records are more similar to bank records than CSLI and consequently fall under the precedent of *Miller*.[187] The court referenced *Smith*, pointing out that just as individuals do not have a privacy interest in the phone numbers they dial—because they are voluntarily disclosing that information to their phone companies—Gratkowski did not have a privacy interest in the information he voluntarily disclosed to Coinbase.[188]

Because it is a financial institution, Coinbase falls under the purview of the Bank Secrecy Act[189] and requires its users to provide their personal information. Because Coinbase collects extensive personal information, using it completely negates the key feature of anonymity of Bitcoin and blockchain technology.[190] As noted, Coinbase's User Agreement specifically states that Coinbase "reserve[s] the right at all times to monitor, review, retain and/or disclose any information as necessary to satisfy any applicable law, regulation, sanctions programs, legal process or governmental request."[191] Thus, the Fifth Circuit was justified in finding that an individual does not have a reasonable expectation of privacy in their Coinbase records.

## C. *Gratkowski*'s Flawed Reasoning

In finding that Gratkowski lacked a privacy interest in his Coinbase records, the Fifth Circuit reasoned that there is a

186 *Id.*

187 *Id.*

188 *Id.* at 311–12.

189 *Id.* Coinbase is licensed as a "money services business," which falls under the regulatory definition of "financial institution," subject to the Bank Secrecy Act. 31 CFR § 1010.100(t); *see also supra* notes 94–95 and accompanying text.

190 *See supra* notes 92–98 and accompanying text.

191 Coinbase User Agreement *supra* note 92.

tradeoff when an individual decides to use a third-party intermediary: The individual gives up privacy—privacy they would otherwise have if they transacted on Bitcoin's blockchain directly—for the ease of using a third-party exchange platform like Coinbase.[192] Notwithstanding this reasoning, the court still found no privacy interest in information located directly on the blockchain, which exists even when an individual uses *no* third-party intermediary.[193] These two findings are inconsistent with one another.

On the one hand, the court reasoned that "Bitcoin users have the option to maintain a *high level of privacy* by transacting without a third-party intermediary."[194] On the other hand, the court reasoned that individuals do not have a legitimate expectation of privacy in their information located directly on the blockchain (i.e., without using a third-party intermediary).[195] This unexplained distinction—that an individual may sacrifice convenience to maintain a "high level of privacy" while simultaneously lacking a "legitimate expectation of privacy"—demonstrates the court's inconsistency in its *Gratkowski* opinion.[196]

Moreover, the court argued that "Bitcoin users are unlikely to expect that the information published on the Bitcoin blockchain will be kept private . . . . [as] it is well known that each Bitcoin transaction is recorded in a publicly available blockchain."[197] While it is true that Bitcoin transactions are publicly announced,[198] this statement demonstrates the

192 *Gratkowski*, 964 F.3d at 312–13 ("Bitcoin users have the option to maintain a high level of privacy by transacting without a third-party intermediary. But that requires technical expertise, so Bitcoin users may elect to sacrifice some privacy by transacting through an intermediary such as Coinbase. Gratkowski thus lacked a privacy interest in the records of his Bitcoin transactions on Coinbase.").

193 *Id.*

194 *Id.* (emphasis added).

195 *See id.* at 312 ("Bitcoin users are unlikely to expect that the information published on the Bitcoin blockchain will be kept private, thus undercutting their claim of a 'legitimate expectation of privacy.'").

196 *Id.* at 312.

197 *Id.* (citing Nakamoto, *supra* note 1, at 2).

198 Nakamoto, *supra* note 1, at 2.

court's misunderstanding of Bitcoin's public disclosure protocol. The court's argument is based on the faulty notion that, since the Bitcoin blockchain is public, users are unlikely to expect that their information will be kept private.[199] However, the reason the Bitcoin blockchain is public refutes the court's logic.

Bitcoin transactions are publicly announced to maintain trust, privacy, and decentralization simultaneously.[200] Bitcoin was created with the goal of establishing a peer-to-peer version of electronic cash, which allows money to be transferred in a decentralized fashion, as in, without a financial institution.[201] The distributed and transparent nature of Bitcoin prevents double-spending and thus preserves trust between transacting parties.[202] This is because the only way to confirm that digital cash has not already been spent, without a trusted third-party, "is to be aware of all transactions."[203]

As for privacy, Bitcoin's cryptographic key system retains anonymity for its users: The public key, also known as the Bitcoin address, is kept anonymous so that it cannot be used to identify the user.[204] Anyone viewing the Bitcoin blockchain "can see that someone is sending an amount to someone else, but without information linking the transaction to anyone."[205] Therefore, the court's reasoning is flawed because it assumes that public announcements make transactions less private,

199 *Gratkowski*, 964 F.3d 307 at 312.

200 *See* discussion *supra* Section II.A.

201 Nakamoto, *supra* note 1, at 1.

202 *See* Nofer et al., *supra* note 25, at 184 ("Using cryptography, people all over the world can trust each other and transfer different kinds of assets peer-to-peer over the internet. . . . [Bitcoin's distributed ledger] increases trust since people do not have to assess the trustworthiness of the intermediary or other participants in the network.").

203 Nakamoto, *supra* note 1, at 2 ("We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions.").

204 *Id.*

205 *Id.* at 6.

whereas Bitcoin's public-private key system preserves anonymity for the transacting parties.

Further, the Fifth Circuit reasoned that the Bitcoin blockchain is more analogous to bank records[206] and telephone logs[207] than CSLI technology.[208] In *Carpenter*, the Supreme Court reasoned that cell phones are unique in that they are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[209] This same logic does not follow to transacting in bitcoin.[210] However, Bitcoin is unique in another way: It was created to retain anonymity for its users.[211] This cannot be said about bank records or telephone call logs. Using Bitcoin, without a cryptocurrency exchange such as Coinbase, does not require the disclosure of any personal information.[212]

Similar to cell-phone location, Bitcoin transactions are not "truly 'shared' as the term is normally understood."[213] Bitcoin transactions are anonymously recorded on the public ledger by nature of its underlying blockchain technology.[214] There is no personal information on the Bitcoin blockchain. The Fifth Circuit's statement that Bitcoin users voluntarily share their information by using Bitcoin to transact[215] contradicts the Supreme Court's reasoning that individuals do not give up their privacy interests in their locations by merely using a cell phone.[216]

206 United States v. Miller, 425 U.S. 435 (1976).

207 Smith v. Maryland, 442 U.S. 735 (1979).

208 Carpenter v. United States, 138 S. Ct. 2206 (2018); United States v. Gratkowski, 964 F.3d 307, 311 (5th Cir. 2020).

209 *Carpenter*, 138 S. Ct. at 2220 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

210 Bitcoin transactions are neither "pervasive" nor "insistent," as there are other means of transacting.

211 *See* Nakamoto, *supra* note 1, at 6.

212 *See supra* Section II.B.

213 *Carpenter*, 138 S. Ct. at 2210.

214 *See* Nakamoto, *supra* note 1.

215 United States v. Gratkowski, 964 F.3d 307, 312 (5th Cir. 2020).

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

Moreover, the court went beyond the facts of the case in finding that an individual does not have a reasonable expectation of privacy in their Bitcoin transactions when transacting without a third party.[217] As discussed in Section II.B, digital wallets provide varying degrees of privacy and control over Bitcoin and a user's personal information. Coinbase provides practically none, desktop and mobile wallets use Tor to prevent the association of payments with IP addresses, and hardware wallets are most secure as they store data offline.[218] A broad interpretation of *Gratkowski* would mean that none of the information stored on digital wallets—or any application of blockchain technology alongside a public disclosure protocol—would be protected by the Fourth Amendment. Due to its inconsistencies, the *Gratkowski* decision is vulnerable to further litigation and should be narrowly interpreted.

## V. THE MODIFIED REASONABLE-EXPECTATION-OF-PRIVACY STANDARD

The *Gratkowski* decision should be interpreted narrowly and with caution. In particular, it should be read to apply only to cases where the defendant uses a centralized cryptocurrency exchange to trade, buy, or sell bitcoin.[219] Such

217 Only after discovering that Gratkowski's public key was associated with a Coinbase account was the government able to subpoena Coinbase for his personal information. *See* Brief of Appellee, *supra* note 163, at 2–3.

218 *See supra* notes 72–76 and accompanying text.

219 As Bitcoin itself is decentralized and anonymous, and there are digital wallets and exchanges that do not require the disclosure of any personal information, it seems that there would be no one to subpoena if not for the presence of a third-party holding information, such as Coinbase. But there are other ways to associate transactions with the identities of a user. First, there are investigative services, such as Cognyte, which "de-anonymizes and reveals illicit transactions made by criminals, thus helping security and law enforcement organizations successfully overcome the challenge of cryptocurrency anonymity." Tom Sadon, *5 Reasons Why Criminals & Terrorists Turn to Cryptocurrencies*, COGNYTE (Nov. 2, 2021), https://www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies/ [https://perma.cc/AT6K-XRME]. These investigative services are often marketed to law enforcement simply because of their

a narrow reading leaves open the question of whether individuals using another platform to transact—decentralized exchanges or other digital wallets—have a reasonable expectation of privacy in their Bitcoin transactions.

One solution is to preserve the third-party doctrine and apply it to Bitcoin exchanges.[220] As this Note discusses in the next Section, such a solution would be proper in situations where the exchange is deemed a "financial institution," as is the case with Coinbase.[221] However, it would be improper to apply such a solution to decentralized exchanges because, unlike centralized exchanges, no single entity retains control over a user's assets.[222] The third-party doctrine applies to information an individual voluntarily discloses to a third-party.[223] When using a decentralized exchange, the only information an individual discloses is the public key or Bitcoin address, information already recorded on the blockchain regardless of the platform used to transact. In other words, an individual using a decentralized exchange does not

effectiveness in combatting and helping to prosecute crime. Some examples include Cognyte, CipherTrace, and CipherBlade. *See, e.g.*, COGNYTE, https://www.cognyte.com/ [https://perma.cc/9448-VU34] (last visited May 10, 2022) ("Over 1,000 government and enterprise customers in more than 100 countries rely on Cognyte's solutions to accelerate security investigations to successfully identify, neutralize, and prevent threats to national security, business continuity, and cyber security.").

220 *See* Christine A. Cortez, *Bitcoin Searches and Preserving the Third-Party Doctrine*, 52 ST. MARY'S L. J. 153, 186 (2020) (arguing that "it is imperative the third party is preserved and only limited on a case-by-case basis").

221 *See supra* notes 93–95 and accompanying text. Moreover, the third-party doctrine properly applies in situations where a defendant voluntarily discloses information to a third-party individual. For example, in *United States v. 89.9270303 Bitcoins*, the district court correctly found that when the defendant "told his wife that she could keep key fob one or give it to Baker and then gave her the passcode to key fob one[,] . . . he relinquished any legitimate expectation of privacy in the fob and its contents because he voluntarily gave the fob and its passcode to third parties." No. SA-18-CV-0998, 2021 WL 4307375, at *10–11 (W.D. Tex., Sept. 22, 2021).

222 Johnson, *supra* note 86, at 37 ("Users deposit their funds directly into a pooled wallet that is controlled by the exchange[.]").

223 Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

voluntarily disclose any identifying information. Thus, the third-party doctrine simply does not extend to a user's identifying information when using a decentralized exchange.

In addition, the third-party doctrine has been criticized by members of the Supreme Court as being ill-suited to the digital age.[224] Justice Gorsuch went so far as to state that the *Carpenter* majority is merely keeping the third-party doctrine "on life support," noting that "countless scholars, too, have come to conclude that the 'third-party doctrine is not only wrong, but horribly wrong.'"[225] Thus, relying on the retention of the third-party doctrine and advocating for courts to apply it to cryptocurrency exchanges is seemingly naïve. Moreover, such a solution is simply inefficient because it cannot be applied uniformly to all digital wallets, but only to those that would fall under the regulatory definition of a "financial institution."[226]

Decentralized exchanges and wallets are not owned by any single entity, nor do they retain custody of any users' assets.[227] Thus, they are not subject to certain standards, such as know-your-customer obligations and anti-money laundering laws.[228] The third-party doctrine applies to information voluntarily disclosed to third parties.[229] Although this doctrine properly applies to centralized exchanges and digital wallets that require disclosure upon registration,[230] it should not apply to those that do not. In other words, the third-party doctrine should not apply to individuals that do

224 *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (stating that the third-party doctrine "is ill-suited to the digital age"); *Carpenter,* 138 S. Ct. at 2262 (Gorsuch, J. dissenting).

225 *Carpenter,* 138 S. Ct. at 2262, 2272 (Gorsuch, J. dissenting) (quoting Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009)).

226 Centralized exchanges such as Coinbase and Kraken are defined as "financial institutions," whereas decentralized exchanges and other digital wallets are not yet defined. Johnson, *supra* note 86, at 37–39.

227 *Id.* at 38.

228 *Id.* at 37.

229 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

230 *See supra* Section IV.B.

not voluntarily disclose identifying information when installing/registering a digital wallet or exchange.

Another proposed solution is to distinguish data by level of control: controlled, semi-controlled, and relinquished.[231] Professor Paul Belonick argues that this distinction reflects the ideals of the Fourth Amendment: control and ownership.[232] Although this is seemingly a fair and viable solution, it is inefficient because it requires substantial inquiry into the specifics of every piece of data in question.[233] The complexity of figuring out how different data is classified, shared, or distributed with every new case may lead to confusion and division among courts. The question should not be whether a given transaction is protected by the Fourth Amendment, but whether an individual's identifying information is protected.

This Note suggests a modified reasonable-expectation-of-privacy standard, supplementing the existing standard with the additional inquiry into what information an individual disclosed in the first place. Such a standard would be most beneficial for its simplicity. To properly apply the test, judges should inquire as to what information an individual disclosed, if any, when installing or purchasing a digital wallet. Considering the variety of digital wallets available, individuals have options when deciding on which wallet to choose.[234] If an individual prefers convenience over anonymity, they will likely opt for a centralized exchange.[235] Conversely, if an individual prefers to remain anonymous, they may opt for the cold storage method, the most secure type of digital wallet available.[236] This solution puts privacy back in the hands of individuals, while simultaneously preserving the integrity of Bitcoin and the Fourth Amendment ideals of ownership, security, and control.

231 Belonick, *supra* note 4, at 177.

232 *Id.* at 178.

233 *See id.*

234 *See supra* Section II.B.

235 *See supra* Section II.C.

236 Frankenfield, *supra* note 74.

The reasonable-expectation-of-privacy test is both subjective and objective.[237] An individual must have a subjective expectation of privacy—an expectation that society is ready to recognize as reasonable.[238] An expectation of privacy is not limited to private places, as "the Fourth Amendment protects people, not places."[239] Indeed, the Supreme Court recognized that what is done in public may still be considered private and protected by the Fourth Amendment.[240] Although Bitcoin transactions are publicly announced, the identities of the parties involved in a given transaction remain anonymous.[241] Applying the Supreme Court's reasoning in *Katz*, what is published on a public blockchain may still be considered private and protected by the Fourth Amendment.[242] The key word here is *may*. The question of whether a user's personal information—identifying information linking them to a transaction—is protected depends on the user's expectation of privacy, an expectation that society recognizes as reasonable.[243]

A user's expectation of privacy in their personal information should depend on what information they disclosed in the first place. Thus, this Note suggests supplementing the existing standard with the additional inquiry into what information an individual voluntarily disclosed when registering/installing a digital wallet or exchange. The current standard would remain the same. However, considering the Supreme Court's repeated warning against the ill-suitability of Fourth Amendment doctrine in addressing privacy concerns arising out of technological advancements, this added inquiry would articulate a proper framework for assessing that standard in the context of Bitcoin and blockchain technology. Moreover, this "modified"

237 *Katz*, 389 U.S. 347, 361 (Harlan, J., concurring).

238 *Id.* (Harlan, J., concurring)

239 *Id.* at 351.

240 *Id.*

241 Nakamoto, *supra* note 1, at 6 (retaining privacy through the anonymity of public keys).

242 *See Katz*, 389 U.S. at 351.

243 *See id.* at 361 (Harlan, J., concurring).

standard—modified in that it is supplemented with the concrete question of what information an individual disclosed—satisfies both the subjective and objective prongs of the reasonable-expectation-of-privacy test.[244] Asking what information an individual disclosed would provide insight into whether the individual had an expectation their identity would be kept private, while simultaneously discerning whether it is an expectation society is ready to recognize as reasonable.

An individual that opts for a centralized exchange, which requires user to provide an array of personal information when registering for the service does not have a reasonable expectation of privacy.[245] If an individual voluntarily discloses all of this identifying information to a private, commercial service, they do not have a reasonable expectation that their personal information will be kept private and protected.

For additional justification, courts may also look to the exchange's user agreements. For example, Coinbase's user agreement stipulates that Coinbase "reserve[s] the right at all times to monitor, review, retain and/or disclose any information as necessary to satisfy any applicable law, regulation, sanctions programs, legal process or governmental request."[246] Thus, individuals who agree to this stipulation give up future Fourth Amendment protections as they relate to their personal information on Coinbase. Moreover, Coinbase defines itself as a money transmitter, putting it under the purview of the Bank Secrecy Act.[247] As it falls under the definition of a "financial institution," Coinbase is regulated as any other financial institution would be regulated under federal law.[248] Similarly, Cash App, another centralized cryptocurrency exchange, stipulates that it can

244 *See id*.

245 *See supra* Section II.C.

246 Coinbase User Agreement, *supra* note 92.

247 *See Legal*, COINBASE, https://www.coinbase.com/legal/licenses [https://perma.cc/ES25-LDUB] (last visited May 10, 2022); *see also* 31 C.F.R. 1010.100(t) (2021).

248 *Id*.

manipulate a user's account if requested by a governmental entity.[249]

On the other hand, an individual that opts for a decentralized exchange does have a reasonable expectation of privacy in their personal information. As noted, unlike centralized exchanges, decentralized exchanges are not controlled by any single entity, they do not maintain control of any user's assets, and they are not subject to the same user-verification obligations.[250] For example, Bisq, a decentralized cryptocurrency exchange, does not require any registration to download and use the service.[251] A new user simply downloads the software onto their computer, without providing any identifying or personal information.[252] Thus, an individual using Bisq does have a reasonable expectation of privacy in their personal information, since they did not voluntarily provide it to any third-party.

This logic can then be applied to individuals using any digital wallet to buy, sell, trade, or store cryptocurrencies.[253] If, upon installation or registration of a digital wallet, an individual provides identifying information, they no longer have a reasonable expectation of privacy in that information.

Digital wallets, private keys, and, especially, hardware wallets may be considered an "effect" as written in the Fourth Amendment, protected in the same way that computers and hard drives are. This issue is beyond the scope of this Note, but it does demonstrate how the Fifth Circuit's finding in *Gratkowski* may hinder appropriate consideration of whether the Fourth Amendment protects Bitcoin transactions.

249 Cash App Terms of Service, CASH APP, https://cash.app/legal/us/en-us/tos [https://perma.cc/3GTL-ADV5].

250 *Supra* notes 99–102

251 BISQ, *supra* note 102 ("Buy and sell [B]itcoin for fiat (or other cryptocurrencies) privately and securely using Bisq's peer-to-peer network and open-source desktop software. No registration required.").

252 *See id.*

253 For a discussion on digital wallets, see *supra* Section II.B.

## VI. CONCLUSION

In *United States v. Gratkowski*, the Fifth Circuit employed reasoning that is both inconsistent and flawed, demonstrating a fundamental misunderstanding of Bitcoin's public disclosure protocol. Moreover, the court went beyond the facts of the case in finding no privacy interest in an individual's Bitcoin transactions, as it is unclear whether the government would have been able to find Gratkowski's personal information had he not been using Coinbase to transact. Thus, *United States v. Gratkowski* should be interpreted narrowly and with caution. Considering Fourth Amendment jurisprudence may be ill-equipped to deal with privacy issues related to Bitcoin, the adoption of a modified reasonable-expectation-of-privacy standard would be an effective way for courts to address privacy issues related to Bitcoin transactions. As Bitcoin's philosophy mimics the Fourth Amendment ideals of security and autonomy, a user's expectation of privacy should depend on the information they voluntarily disclose when registering for a digital wallet.