Transparency is the New Privacy: Blockchain's Challenge for the Fourth Amendment

Paul Belonick[*]

23 STAN. TECH. L. REV. 114 (2020)

ABSTRACT

Blockchain technology is now hitting the mainstream, and countless human interactions, legitimate and illegitimate, are being recorded permanently—and visibly—into distributed digital ledgers. Police surveillance of day-to-day transactions will never have been easier. Blockchain's open, shared digital architecture thus challenges us to reassess two core premises of modern Fourth Amendment doctrine: that a "reasonable expectation of privacy" upholds the Amendment's promise of a right to be "secure" against "unreasonable searches," and that "a reasonable expectation of privacy" is tantamount to total secrecy. This article argues that these current doctrines rest on physical-world analogies that do not hold in blockchain's unique digital space. Instead, blockchain can create security against "unreasonable searches," even for data that are shared or public, because blockchain's open distributed architecture does the work in digital space that privacy does in physical space to advance Fourth Amendment values such as security, control of information, free expression, and personal autonomy. The article also evaluates

[*] Assistant Prof. of Practice and Director, Startup Legal Garage, Center for Innovation, UC Hastings Law School. University of Virginia, J.D. 2010, PhD. 2016. I would like to thank Robin Feldman, Darryl Brown, Ric Simmons, Jonathan Widmer-Rich, Andrew Crespo, David Roberts, and the participants of the CrimFest! 2019 conference for their advice and comments. Maximilien Pallu, Cyril Kottuppallil, and Katie Lindsay provided excellent research assistance. My wife provided much needed support.

textualist approaches to blockchain, concluding that the twenty-first century's latest technology shows how the eighteenth-century text's focus on ownership and control may be a better means to achieve fundamental human ends than privacy-as-secrecy. Finally, the article proposes an analytical framework for Fourth Amendment protections for distributed ledgers—corresponding to the levels to which blockchain users evince control of their data—that is grounded in text and theory and that is administratively practicable for courts.

TABLE OF CONTENTS

INTRODUCTION

Bitcoin. Drugs and the dark web. But also that flashy TV ad you just saw?[1] You've probably heard a lot about blockchains recently. Proponents proclaim that blockchains will create frictionless exchanges of information and value that will

[1] *See, e.g.*, *IBM Cloud Blockchain TV Commercial, "The Blockchain Built for Smarter Business,"* ISPOT.TV (2018), https://perma.cc/7YY8-PFNF.

transform economies, governments, and perhaps all human relations.[2] Others, of course, are rightly skeptical,[3] but nonetheless see blockchain's vast and growing potential.[4] That potential is currently being realized: dozens of proposed and functioning use cases for blockchains are extant, from storage to smart contracts to digital publishing to finance to Internet-of-Things data collection,[5] while businesses, governments, and major industries in multiple sectors are considering and adopting blockchains into their recordkeeping systems,[6] or are accepting

[2] *See, e.g.* KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 91 (2018) [hereinafter WERBACH, BLOCKCHAIN] ("In time, systems based on blockchain technology's foundational innovations could influence all aspects of business, government, and human communities. It would be premature to label the blockchain a revolution with similar impacts as the printing press, the telephone, or the Internet, but it belongs in the same conceptual category."); Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, 95 Harv. BUS. REV., Jan.-Feb. 2017, at 118, 120 ("With blockchain, we can imagine a world in which . . . [i]ntermediaries like lawyers, brokers, and bankers might no longer be necessary. Individuals, organizations, machines, and algorithms would freely transact and interact with one another with little friction."); Susanne T. Tempelhof & James F. Tempelhof, *BITNATION Pangea: The World's First Virtual Nation—A Blockchain Jurisdiction*, GLOBAL CHALLENGES FOUND. (Nov. 30, 2016), https://perma.cc/Z8JW-HSKR (arguing that blockchain may "fundamentally replace the Nation State"). The hype can grow absurd. *See, e.g.*, Arie Shapira & Kailey Leinz, *Long Island Iced Tea Soars After Changing Its Name to Long Blockchain*, BLOOMBERG (Dec. 21, 2017), https://perma.cc/8KTL-HFR4. Such bandwagoning has spawned the derisive term "chainwashing." WERBACH, BLOCKCHAIN, *supra*, at 72, 266 n.8.

[3] WERBACH, BLOCKCHAIN, *supra* note 2 at 3, ("[Blockchain] is the subject of boundless enthusiasm, much of it wildly uninformed. . . . It could change the world . . . but crucially, how and when remain uncertain."); DYLAN YAGA ET AL., NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T COMMERCE, BLOCKCHAIN TECHNOLOGY OVERVIEW (2018) ("It is not magical; it will not solve all problems. As with all new technology, there is a tendency to want to apply it to every sector in every way imaginable.").

[4] *See, e.g.*, Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH L.J. 487, 489, 490-91 (2017) [hereinafter Werbach, *Trust, but Verify*] ("While the near term impacts of the blockchain may be overhyped, its long-term potential as a distributed foundation for the exchange of value is extraordinary."). Recall also futurist Roy Amara's aphorism: "We tend to overestimate the impact of technologies in the short run but underestimate them over the long term." WERBACH, BLOCKCHAIN, *supra* note 2 at 245.

[5] *See, e.g.*, PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 119-22 (2018) (describing data storage use cases); Kaspars Zīle & Renāte Strazdiņa, *Blockchain Use Cases and Their Feasibility*, 23 APPLIED COMPUTER SYS. 12, 12-13 (2012) (collecting blockchain use case studies); Scott J. Shackelford, *Governing the Internet of Everything*, 37 CARDOZO ARTS & ENT. L.J. 701, 725 (2019) (noting the promises of and challenges facing Internet of Things blockchain applications). On the Internet of Things, see generally Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 76, 805, 812-25 [hereinafter Ferguson, *IoT*].

[6] *See, e.g.*, AM. COUNCIL FOR TECH.—INDUS. ADVISORY COUNCIL, ENABLING BLOCKCHAIN INNOVATION IN THE U.S. FEDERAL GOVERNMENT: A BLOCKCHAIN PRIMER 34 (2017) [hereinafter ACT-IAC, ENABLING BLOCKCHAIN INNOVATION] (describing possible government applications

cryptocurrencies.[7] Scholars are therefore pondering the legal implications of blockchain's sudden onset. Previous law review articles on blockchain have largely focused on securities regulation and copyright,[8] and have more explained what blockchain generally tries to do than how exactly it works.[9] This article's focus is different: to assess how blockchain and its technical elements interact with the Fourth Amendment.

Begin with the technology: blockchain is a novel digital architecture for data storage, control, and access.[10] It is a distributed, collective, and (usually) publicly visible ledger that permits multiple parties who may not trust (or even know) each other to share and publish information securely, without a central organizing authority and with very little fear of fraud, data loss, or tampering because of the extraordinary difficulty of changing data on the ledger.[11] Many readers will be aware that blockchains are used for cryptocurrencies, such as bitcoin,[12] Monero, ZCash, and now Facebook's Libra.[13] Indeed, blockchain was invented to create

for blockchain systems); Chris Isidore, *JPMorgan Is Creating Its Own Cryptocurrency*, CNN BUS. (Feb. 14, 2019), https://perma.cc/W9H9-8A9Q; DELOITTE, BREAKING BLOCKCHAIN OPEN: DELOITTE'S 2018 GLOBAL BLOCKCHAIN SURVEY 19 (2018) (in survey of executives in companies with over $500 million in revenue, 69% of respondents said they are planning to replace some current record systems with blockchain).

[7] *See, e.g.*, Elise Moreau, *13 Major Retailers and Services that Accept Bitcoin*, LIFEWIRE (Nov. 4, 2019), https://perma.cc/2CU6-CAUZ (noting Overstock.com, Dish Network, Microsoft, Reeds Jewelers, and others); Tamara Chuang, *Denver Flyers Can Now Use Bitcoin When Parking at ParkDIA*, DENVER POST (Apr. 19, 2017), https://perma.cc/LPM9-66HL; Ronald D. Rotunda, *Bitcoin and the Legal Ethics of Lawyers*, VERDICT (Nov. 6, 2017), https://perma.cc/A2EP-EGWF (discussing ethics of lawyers' accepting cryptocurrencies).

[8] Scott J. Shackelford & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology To Build Trust and Promote Cyber Peace*, 19 YALE J.L. & TECH. 334, 337 n.9 (2017) (noting common areas of academic study of blockchain uses).

[9] For exceptions, with highly detailed descriptions of the technology, see, e.g., *id.* at 383-88; Wulf A. Kaal & Craig Calcaterra, *Crypto Transaction Dispute Resolution*, 73 BUS. LAW. 109, 109, 110-24 (2018).

[10] *See* YAGA ET AL., *supra* note 3.

[11] *Id.*; Petter Hurich, *The Virtual Is Real: An Argument for Characterizing Bitcoins as Private Property*, 31 BANKING & FIN. L. REV. 573, 576 (2016). Because blockchain technology is so new, there are no set definitions for much of its nomenclature. Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 REV. BANKING & FIN. L. REV. 713 (2017). I have tried to use apparently common terminology.

[12] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN (2009), https://perma.cc/4883-DP48. Note that bitcoin refers to the currency, while Bitcoin refers to the blockchain protocol and network that run the currency. WERBACH, BLOCKCHAIN, *supra* note 2, at 14.

[13] REG'L ORGANIZED CRIME INFO. CTR., BITCOIN AND CRYPTOCURRENCIES: LAW ENFORCEMENT INVESTIGATIVE GUIDE 6-7 (2018) [hereinafter ROCIC, BITCOIN AND CRYPTOCURRENCIES] (listing characteristics of major cryptocurrencies); ROBBY HOUBEN & ALEXANDER SNYERS, CRYPTOCURRENCIES AND BLOCKCHAIN: LEGAL CONTEXT AND IMPLICATIONS

and record bitcoin transactions, which is why blockchain is often confused with Bitcoin.[14]

But blockchain isn't a currency; it is the digital infrastructure or protocol that can support digital currency transactions, as well as scores of other purposes. Blockchains are particularly useful when many people want to record information as a group without any one person controlling the data.[15] For instance, Toyota is exploring blockchain solutions for coordinating and recording the vast amount of information that the many industries involved in building autonomous vehicles will generate.[16] The energy sector is building blockchains to record energy delivery and sales among multiple parties.[17] And assorted industries are forming blockchain consortia to oversee advertising data.[18]

A student of the Fourth Amendment will immediately sense something important here. Those autonomous vehicle blockchains will record where we've been; energy blockchains will permanently log when our lights were on; advertising blockchains will track what we bought and searched for. Like GPS trackers,[19] smart phones,[20] and cell phone towers,[21] blockchains create, store, and share tremendous amounts of information of various kinds—which will inevitably become of interest to criminal investigators. That's not because, as the stereotype goes, cryptocurrencies are for criminals.[22] Rather, as cryptocurrency

FOR FINANCIAL CRIME, MONEY LAUNDERING AND TAX EVASION 51 (2018) (same); Josh Constine, *Facebook Announces Libra Cryptocurrency: All You Need To Know*, TECHCRUNCH (Jun. 18, 2019), https://perma.cc/Z7B6-6E9N.

[14] Matt Lucas, *The Difference Between Bitcoin and Blockchain for Business*, BLOCKCHAIN PULSE (May 9, 2017), https://perma.cc/JW85-ZPBH.

[15] *See, e.g.*, Karl Wüst & Arthur Gervais, *Do You Need a Blockchain?*, 1ST CRYPTO VALLEY CONF. ON BLOCKCHAIN 45 (2018).

[16] Emma Sandler, *Toyota Doubles Down on Blockchain Tech for Autonomous Vehicles*, AUTO FIN. NEWS (May 23, 2017), https://perma.cc/JTC7-ALNQ; Gerald Fenech, *The Link Between Autonomous Vehicles and Blockchain*, FORBES (Oct. 30, 2018), https://perma.cc/8C4R-ZLM4 (describing how blockchain "helps to eliminate barriers preventing companies from positively interacting with each other" to further autonomous vehicle development).

[17] James Basden & Michael Cottrell, *How Utilities Are Using Blockchain To Modernize the Grid*, HARV. BUS. REV. (Mar. 23, 2017), https://perma.cc/W7XR-RLRV.

[18] Press Release, Mediaocean & IBM, Mediaocean and IBM Partner To Integrate Blockchain Across the Media Ecosystem; New Blockchain Consortium Includes Kellogg, Kimberly-Clark, Pfizer and Unilever (Jun. 19, 2018), https://perma.cc/UA6Z-BCX3.

[19] United States v. Jones, 565 U.S. 400 (2012).

[20] Riley v. California, 573 U.S. 373 (2014).

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

[22] That stereotype is past its prime. Wilma Woo, *U.S. DEA "Actually Wants" Criminals to Keep Using Bitcoin*, BITCOINIST (Aug. 8, 2019), perma.cc/G4MC-ARAL (noting DEA research showing that "the percentage of Bitcoin transactions tied to criminal activity had dropped from 90 percent in 2013 to just 10 percent in 2018").

uses become more widespread, and especially as big enterprises turn to blockchains, millions of everyday actions will be recorded onto blockchains, leaving digital traces of what people exchanged, places they went, and with whom they interacted. But unlike in mere traditional databases, those traces will remain there forever, immutable, and—to varying degrees—publicly accessible and visible.[23]

How should courts, law enforcement, litigants, and scholars react? Fourth Amendment doctrine—naturally rooted in physical places, containers, and actions—has famously struggled to translate neatly from physical to digital space, even as concerns about technology and Big Data collection have grown.[24] Blockchain is part of that Big Data collection revolution, and carries the privacy concerns that such collection raises. But it is also sui generis, and subverts or resists easy analogy to the physical world. Blockchain's distributed, secure, immutable, and censorship-resistant structure rests—counterintuitively—on its data's being *shared* and *publicized* among various users.[25] There is no master copy, and the ledger does not physically exist in just one place.[26] It is a store of information, but also a medium of value and exchange.[27] And it is "at heart a cryptographic protocol" that can permit a ledger's data to be public and visible while masking the identities of the ledger's users through algorithmic privacy mechanisms more potent than any physical lock or wall.[28]

These unique characteristics radically challenge the core premises of modern Fourth Amendment doctrine: that *privacy* upholds the right to be "secure" against unreasonable searches, and that "a reasonable expectation of privacy" is tantamount to *secrecy*.[29] The technology particularly unsettles the physical-world rationales that underpin classical Fourth Amendment rules such as the public/non-public and content/non-content distinctions and the third-party and false-friend doctrines.[30] Blockchain forces us to recognize that privacy and secrecy are often instruments to other vital human ends, and that technology can distort or render obsolete those instruments and also the legal doctrines that flow

[23] ROCIC, BITCOIN AND CRYPTOCURRENCIES, *supra* note 13, at 15; *see also* Woo, *supra* note 22.

[24] *See generally* Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 533, 553-54 (2017).

[25] *See infra* Part II.D.

[26] Jean Bacon et al., *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers*, 25 RICH. J.L. & TECH. 21, 21-22 (2018).

[27] *See* YAGA ET AL., *supra* note 3, at iv-v.

[28] Michael Nielsen, *How the Bitcoin Protocol Actually Works*, DATA-DRIVEN INTELLIGENCE (Dec. 6, 2013), https://perma.cc/9RNG-EHL7 [hereinafter Nielsen, *Bitcoin Protocol*].

[29] *Infra* Part III.A.

[30] *Infra* Part III.D.1.

from them. We must resolve the resulting paradoxes, however, to provide for both reasonable civil liberties and reasonable opportunities to investigate crime.[31]

This article is the first to attempt to sort out those paradoxes, just at a time when blockchain is going mainstream. Because the technology is still new, there are few reported prosecutions involving blockchains. So far, courts have hinged motions to suppress in those cases on issues apart from the technology itself.[32] But with blockchains on their way, this article attempts to anticipate—with hardy reservations about blockchain enthusiasts' wilder prognostications—the doctrinal challenges that blockchains will present.

Part I of this article describes the theoretical background of blockchain, with an eye towards later Fourth Amendment analysis, and shows how blockchain is a technology imbued with philosophical goals and concerns about security, human autonomy, and free expression. Part II describes several aspects of the technology itself, and shows how the technology actually instantiates blockchain's philosophy.[33] Part III analyzes Fourth Amendment doctrine through the lens of blockchain and its theoretical background. It shows that some aspects of blockchain—the private key, the digital wallet—may fit into a "reasonable expectation of privacy." But it also shows that blockchain's philosophy furthers numerous scholarly critiques of current Fourth Amendment jurisprudence. Blockchain's open architecture undermines the Supreme Court's current conception of a "reasonable expectation of privacy" as "privacy-as-secrecy" while advancing alternative views of privacy and alternative values—including security from government intrusion, free expression in conjunction with the First Amendment, and personal autonomy—that numerous scholars have suggested the Fourth Amendment protects. These values are implicit in the control of data that blockchain permits, but privacy-as-secrecy cannot vindicate them. Part III also considers a textualist test: a "search" of a blockchain would occur when officers invade a user's secure "papers"—here blockchain data—and would be "unreasonable" if so sweeping as to resemble the Fourth Amendment's original *bête noir*, the general warrant. Part III shows as well how blockchain concretizes

[31] *See* Werbach, *Trust, but Verify*, *supra* note 4, at 495-96 (noting that blockchain cannot "displace traditional law entirely").

[32] As of August 3, 2019, the Westlaw search string ((bitcoin or block-chain or blockchain or "distributed ledger" or "shared ledger" or Ethereum or crypto-currency or cryptocurrency or "digital currency" or "digital token") and ("4th Amendment" or "Fourth Amendment" or "motion to suppress")) results in 24 cases, all of which relate tangentially to blockchain or center on warrant-searches of individual computers, and courts in these cases seem eager to find familiar grounds on which to rule, rather than wade into new technology. *See, e.g.*, United States v. Ulbricht, 14-CR-68 KBF, 2014 WL 5090039, at *15 (S.D.N.Y. Oct. 10, 2014), *aff'd*, 858 F.3d 71 (2d Cir. 2017) (not considering "novel" highly technical arguments).

[33] *Infra* Part II. *See generally* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003) (noting that Fourth Amendment analyses can shift depending on how closely courts focus on how a technology actually works versus how the public thinks it works).

the notion that intangible computer data are "effects" for Fourth Amendment purposes, and can suffer trespassory searches. Control again is key. Finally, Part IV provides a way forward through the doctrinal thicket, arguing that the Fourth Amendment can restrict government examination in criminal investigations of open, shared blockchain data, and proposes a framework for doing so. Recognizing that control of data, not privacy, best achieves the Fourth Amendment's text and goals on a blockchain, it suggests a distinction between publicly relinquished blockchain data, semi-controlled data, and fully controlled data, which would correspond, respectively, to "non-searches," "reasonable-suspicion" searches, and full probable-cause searches requiring a warrant.[34]

I. THE PHILOSOPHY OF BLOCKCHAIN: SECURITY, CONTROL, AND DIGITAL SPACE

Consider an age-old human problem: how do we navigate a world filled with untrustworthy people who want to do us or our valuables harm? In the physical world, fear of untrustworthy others spurs us to seek security through several means. Fourth Amendment doctrine has at various points considered these means of security in the physical world, affording legal protections to some but not others. One means to keep things secure in the physical world is to hide them. The reason is simple: if a physical thing that we want to keep *secure* is kept *secret*, we can reasonably expect that untrustworthy people will not know about it and will be less able to take or damage it. If the thing is *hidden* in our house, we can reasonably expect to exercise close control over it. If we keep a bit of information quiet, there is less chance that untrustworthy people will manipulate it or use it to harm us. We can also add to the security of hiding things by enclosing them out of the sight of others and locking them.[35] In the physical world, obscurity (i.e., concealment) helps lead to security.

A second way to gain security is to surround ourselves with acquaintances whom we trust not to hurt us, what we can call "Peer-to-Peer" or "P2P" trust systems.[36] It is generally easy to enforce trust (and thus effect security for information and exchange) among small groups of people who know each other.[37] We might give to trusted parties access to places or items that we do not give to

[34] This article analyzes only Fourth Amendment search doctrine, and not how blockchain's architecture might upend seizure doctrine or the warrant particularity requirement, or how privacy statutes might affect blockchains—tasks for another day.

[35] *See* Jakob Nielsen, *Usability 101: Introduction to Usability*, NIELSEN NORMAN GROUP (Jan. 3, 2012), https://perma.cc/DU3H-D3EH [hereinafter Nielsen, *Usability*] ("In the world of atoms we achieve security with devices such as locks, safe, signatures, and bank vaults.").

[36] WERBACH, BLOCKCHAIN, supra note 2, at 25-26.

[37] *See, e.g.*, Lisa Bernstein, *Private Commercial Law in the Cotton Industry: Creating Cooperation Through Rules, Norms, and Institutions*, 99 MICH. L. REV. 1724, 1749-50 (2001).

strangers. But trust grows weaker, and reasonable expectations about whom to trust shift, as the group expands and face-to-face social pressures wane.[38]

A third important means by which we seek security from untrustworthy people in the physical world is to resort to trusted intermediary third parties. That includes ceding some control over our affairs to legal systems that act as proxies and enforcement mechanisms for the trust that we cannot fully place in others. This resort has been called the "Leviathan" system of trust, a reference to a Hobbesian enforcement of social order through state sanctions.[39] Similarly, especially in the modern world, we often resort to large private intermediaries to enforce trust.[40] Banks are a good example: they keep track of money in accounting ledgers that keep anyone from trying to "double-spend" the same dollar, or from issuing checks from empty accounts.

Experience with these problems and solutions, of course, informs much of traditional Fourth Amendment theory and doctrine. Scholars have argued that Fourth Amendment protection against government intrusion equates (or should equate) with positive or common law mechanisms that provide security against private parties, mechanisms rooted in physical space.[41] For instance, courts have strongly privileged obscurity-as-security when analyzing Fourth Amendment protections,[42] while they all but erased private third-party and (to a lesser extent) P2P trust from the Fourth Amendment picture—although there are strong signs that that may be changing.[43]

But these problems and solutions translate imperfectly at best to the digital world. Take "obscurity-as-security": internet data generally travel between computers along non-obscured, even "unsecured [electronic] channels, making them vulnerable to interception."[44] To try to counter this fact, computer scientists have developed nigh-uncrackable methods to encrypt information, beyond any protection a lock could ever give, but this work-around cannot fully replace (and even reduces) trust.[45] We will detail these methods below.[46]

P2P trust transfers particularly poorly: on anonymous networks dispersed across the planet, opportunities for self-dealing become pervasive, and the ability to maintain order through mere social pressure drops precipitously.[47] Meanwhile,

[38] *Id.* at 1750-51.

[39] WERBACH, BLOCKCHAIN, *supra* note 2, at 27.

[40] *Id.* at 27-28.

[41] *Infra* Part III.B. *See generally* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821 (2016).

[42] *Infra* Part III.A-B.

[43] *Infra* Part III.D.1.iii.

[44] DE FILIPPI & WRIGHT, *supra* note 5, at 14.

[45] *Id.* at 14-15.

[46] *See infra* Part II.E.

[47] WERBACH, BLOCKCHAIN, *supra* note 2, at 27, 35, 39.

costs of lost trust rise: network operators and businesses have to construct extensive security mechanisms to prevent hacking and fraud,[48] and merchants must demand large amounts of sensitive personal information from digital customers to trust them as trading partners.[49] For all that, a certain amount of fraud must still be tolerated and its costs externalized to all network participants.[50]

Finally, "Leviathan" trust moves inconsistently from physical to digital space, for both socio-political and practical reasons. Centralized authority—as the authors of the Constitution and Bill of Rights knew well—can be as much a threat as an aid to citizens' security, and centralized digital power can reach far more invasively than physical power ever could.[51] As early as the 1980s and into the 1990s, at the dawn of the internet, computing enthusiasts with a libertarian bent were bruiting fears that governments and corporations with vast access to personal data could easily invade individual privacy and erode personal liberty.[52] The far-reaching control that some nations[53]—to say nothing of Facebook and Google[54]—can now exercise over digital data may confirm the prescience of these worries. Among these concerns was that governments could repress and censor digital information and seek out dissidents who published it.[55] Meanwhile, the dot-com bubble burst of the early 2000s and the financial crisis of 2008 further degraded trust in third-party institutions and the data systems on which they operated.[56] Bitcoin's inventor(s), a person or persons operating under the pseudonym "Satoshi Nakamoto,"[57] evidently shared this dim view of powerful

[48] *See* Claudia Loebbecke et al., *Blockchain Technology Impacting the Role of Trust in Transactions*, 26TH EUR. CONF. ON INFO. SYS. 5-7 (2018).

[49] Nakamoto, *supra* note 12, at 1.

[50] *Id.*

[51] *Infra* Part III.A.

[52] *See, e.g.*, David Chaum, *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, 28 COMM. ACM 1030 (1985); Eric Hughes, *A Cypherpunk's Manifesto*, ACTIVISM.NET (Mar. 9, 1993), https://perma.cc/AD7H-J6MM; John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (1996), https://perma.cc/5BCU-RYZE (claiming that governments "have no sovereignty where we gather"); WERBACH, BLOCKCHAIN, *supra* note 2, at 5 (noting that blockchain was "initially championed by radical technolibertarians.").

[53] *See generally* EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM (2011) (describing authoritarian regimes' control of the internet); Werbach, *Trust, but Verify*, *supra* note 4, at 521 (describing China's "Great Firewall").

[54] Werbach, *Trust, but Verify*, *supra* note 4, at 509-10; Donohue, *supra* note 24, at 614; Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1916-17, 1923 (2013).

[55] *See, e.g.*, *Internet Censorship Newest Threat to Press Freedom*, FREEDOM HOUSE (Apr. 17, 2000), https://perma.cc/V6SC-PWX8.

[56] WERBACH, BLOCKCHAIN, *supra* note 2, at 35-39.

[57] The identity of "Satoshi Nakamoto" is still unknown. *Satoshi Nakamoto*, BITCOIN WIKI, https://perma.cc/4883-DP48 (archived Dec. 28, 2019).

state and financial incumbents, famously encoding into the first bitcoin block a newspaper headline: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."[58] The logical desideratum was some form of censorship-resistant data storage that could not be manipulated or controlled by Leviathan-type entities.[59]

But even setting aside pyretic warnings of digital tyranny, there are pragmatic reasons to be timid about placing trust in centralized digital authorities: such institutions have repeatedly proven inept as central points of data storage and reconciliation. Internet companies have long been "predominantly structured using a 'client-server' model," in which a server hosts and stores various data and passes the data directly to customers.[60] Servers are thus centralized points of data collection that can act as "single points of failure" apt to crash (making their data unavailable) if overwhelmed by users or attacked.[61] Moreover, as noted, asking companies to act as trust proxies requires them to collect sensitive information about customers—information, as is well known, that regularly falls prey to hackers.[62]

Thus, the transition from physical to digital world brought new twists on the age-old problem of security: anonymous counterparties, vulnerable centralized servers, hacking, mass information collection, and malign motives (or at least incompetence) of large institutional actors that would otherwise merit confidence. Physical solutions need considerable reworking for this environment. Blockchain technology responds to these concerns, promising a system of data exchange that would replace or reconfigure antidotes to untrustworthiness in the physical world with antidotes for the digital world.[63] In doing so, it upends traditional ways of thinking about security and privacy. To see how, let's turn to how blockchains work.

[58] WERBACH, BLOCKCHAIN, *supra* note 2, at 42.

[59] *Id.* at 150, 152 (noting the argument that "[c]ensorship resistance . . . is the sine qua non of blockchain-based systems").

[60] DE FILIPPI & WRIGHT, *supra* note 5, at 16-17; Mariem Hammani, Bitcoin: Blockchain Mechanism 5 (March 2017) (unpublished manuscript), https://perma.cc/9G9W-XLX5.

[61] DE FILIPPI & WRIGHT, *supra* note 5, at 16-17.

[62] Examples are legion. See, e.g. *2019 Data Breaches—The Worst So Far*, IDENTITYFORCE (Jan. 3, 2019), https://perma.cc/CDX3-W8AQ.

[63] *See generally* Nakamoto, *supra* note 12; Nielsen, *Bitcoin Protocol*, *supra* note 28 ("[T]he problems Bitcoin needs to solve are largely about securing transactions—making sure people can't steal from one another, or impersonate one another, and so on.").

II. HOW DOES IT WORK?

Blockchain is highly technical, and a discussion of all its aspects is impossible here.[64] I want instead to focus on five of its technical features that instantiate the philosophical goals and concerns described in the previous section and that most directly touch Fourth Amendment issues. First, three computer science concepts that underlie the blockchain architecture: the cryptographic hash, asymmetric public-private key cryptography, and the digital signature. Next, blockchain's transparent, publicly visible decentralized exchange between strangers that is secure and practically impossible to tamper with once made, which the hash, asymmetric cryptography, and digital signatures make possible. Finally, its pseudonymity, which permits parties to exchange openly yet privately at once. These features, in sum, collectively and counterintuitively use transparency and sharing to upend and replace traditional security-through-obscurity and P2P and "Leviathan" trust. We'll discuss all these features in the context of transactions between two blockchain users, "Alice" and "Bob."

A. The Cryptographic Hash

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.[65] This conversion is called "hashing." The resulting string is called a "digest."[66] 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.[67] Thus, if Alice wants to secure some data, she can hash it. An interloper who might see this jumbled string could, in theory, try to reverse-engineer the digest by sheer trial and error, known as a "brute force attack."[68] But with modern digests up to 512 bits long and possible underlying permutations into the trillions of trillions, the computing energy and time necessary for such trial and error is unfathomable: enormous supercomputers could not manage it

[64] For a good visual explanation of how blockchain works, see Maryanne Murray, *Blockchain Explained*, REUTERS (June 15, 2018), https://perma.cc/N9VQ-X5ZR.

[65] For example, hashing the plaintext phrase "Hello, world!0" through SHA-256, a common hash algorithm, yields the digest 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64. Nielsen, *Bitcoin Protocol*, *supra* note 28.

[66] YAGA ET AL., *supra* note 3, at 7.

[67] Hashing the slightly altered text "Hello, world!1" through the same algorithm as in note 82 produces the digest e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8. Nielsen, *Bitcoin Protocol*, *supra* note 28.

[68] Patrick Nohe, *How Strong Is 256-Bit Encryption?*, HASHEDOUT (May 2, 2019), https://perma.cc/FKW4-D934.

even in *billions* of years.[69] That kind of security is unparalleled in the physical world.

B. Asymmetric Public-Private Key Cryptography

A cryptographic "key" function is similar to a hash, but a hash only scrambles data, while a key can scramble and unscramble.[70] "Key," of course, is a metaphor. A cryptographic key doesn't "open" anything like in the physical world. Rather, keys are long strings of characters that act as variables in algorithms.[71] The algorithms process the variables and the data to be scrambled to generate long strings like hash digests. So if Alice wants to send some data securely to Bob, she can run it through a key function and then send the digest securely even over an open network. If Bob has a paired key, he can *un*scramble the encrypted data back into readable text.

Now, in this simple "symmetric" system, Alice and Bob share a single key variable that can be used to scramble and unscramble.[72] But Alice needs to trust Bob never to share the key with unauthorized others or to use it to unscramble her transactions with other people. Moreover, if she sends a key *itself* over an open network to share with Bob, an interloper might intercept it.[73] Symmetric, one-key systems cannot replace trust on a large network.

The solution is an "asymmetric" system.[74] This 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. The two keys are created and linked by a mathematical algorithm,[75] and the public key scrambles data, while only the private key can unscramble the data.[76] Trillions of numerical permutations could

[69] "[A] 256-bit [digest] will have 115,792,089,237,316,195,423,570,985,008,687,907, 853,269,984,665,640,564,039,457,584,007,913,129,639,936 [78 digits] possible combinations. No Super Computer on the face of this earth can crack this. Even if you use Tianhe-2 [MilkyWay-2], the fastest supercomputer in the world, it will take millions of years to crack the 256-bit encryption." *Id.* at 2; YAGA ET AL., *supra* note 3, at 8 (noting that it would take trillions of years for hash algorithms to produce the same hash from different inputs).

[70] *What is The Difference Between Hashing and Encrypting*, SECURITY INNOVATION EUROPE BLOG (Oct. 31, 2016), https://perma.cc/TJA4-GXN9.

[71] For examples of key strings, see phpseclib: RSA Examples and Notes, PHPSECLIB, https://perma.cc/95JF-R9ZS (archived Dec. 26, 2019).

[72] YAGA ET AL., *supra* note 3, at 11.

[73] DE FILIPPI & WRIGHT, *supra* note 5, at 14.

[74] First proposed by R.L. Rivest et al., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 21 COMM. ACM 120 (1978).

[75] For a simplified explanation of the math, see *Public Key Encryption*, TUTORIALSPOINT, https://perma.cc/7JRH-WLD5 (archived Dec. 26, 2019).

[76] Alternatively, the private key can encrypt and the public key decrypt. YAGA ET AL., *supra* note 3, at 11.

create the public/private key pair, and brute force attacks on the public key to reverse-engineer its private key are, as for hashes, hopeless.[77]

In a two-key system, if Alice wants to send some data to Bob she scrambles the data using Bob's public key (which she can request or find openly available on the network), then sends the encrypted data to Bob. Bob's private key algorithm alone can unscramble the encrypted data. Alice and Bob never have to share both keys. They share only the public key. They can thus share data privately over public networks, fully assured that no one else can interfere, even if the world can see scrambled data passing.[78]

Now, as its name suggests, the private key must be kept private, or others will be able to unscramble messages sent with the paired public key.[79] Users could write the key down on paper manually, but often use secure servers or offline storage or key-holding secure "escrow" services.[80] 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.[81] "Wallets" will be part of our Fourth Amendment analysis below.[82]

C. *The Digital Signature*

This concept follows from asymmetric key cryptography, and undergirds blockchain's defense against untrustworthy strangers on the internet. Suppose Bob gets an electronic message from "Alice" offering to enter into an exchange of some data, perhaps a transfer of a bitcoin. Bob can verify on an open blockchain ledger—we'll discuss in a moment how he does so—that a user named "Alice"[83]

[77] That is, for now. Much-anticipated "quantum computing" methods may in time be able to brute-force cryptographic keys. That is currently not the situation, however. Jack Kelly et al., Investigation of Blockchain Network Security (May 17, 2018) (unpublished manuscript), https://perma.cc/9Q3M-AXF5.

[78] ROCIC, BITCOIN AND CRYPTOCURRENCIES, *supra* note 13, at 3 ("Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers makes it impossible to break this scheme. A Bitcoin address is more secure than Fort Knox.").

[79] Bacon et al., *supra* note 26, at 22.

[80] YAGA ET AL., *supra* note 3, at 13. Such escrow services often must satisfy Know-Your-Client requirements. Bacon et al., *supra* note 26, at 22. Offline key storage is known as "cold" storage, while online storage is known as "hot" storage. Houben & Snyers, *supra* note 13, at 17.

[81] ROCIC, BITCOIN AND CRYPTOCURRENCIES, *supra* note 13, at 15; Hammani, *supra* note 60, at 23. "Wallet" is yet another tricky metaphor. Kelly et al., *supra* note 77, at 2 ("[T]he cryptocurrency 'wallet' is really a misnomer designed to make transactions easier to understand, as there is no actual wallet anywhere. When a company like Coinbase says they are storing your Bitcoin in your wallet, this is being accomplished by storing a set of Elliptic Curve Digital Signature Algorithm [ECDSA] public and private key pairs.").

[82] Part III.B.

[83] On a real blockchain, "Alice" would be known by a pseudonymous address. *Infra* Part II.E.

owns the coin offered. But how can Bob know for sure that this same "Alice" is offering the coin, and not some scammer using Alice's name?

The public/private key pair can be used to "sign" digital exchanges. To prove her identity, Alice runs the offered data through Bob's public key to encrypt it, resulting in a "data" digest. Then Alice runs same data through her own *private* key, resulting in a second, "signature" digest. She then sends the resulting data digest and encrypted signature digest to Bob. Bob can unscramble the data digest with his private key. Once he has the unscrambled data, he goes on the network, finds the user "Alice's" *public* key, and runs the unscrambled data through it. If the result is the same as the signature digest he got from Alice, it is mathematically all but certain (assuming of course, that Alice's private key has never been stolen) that the user "Alice" is the same person who also ran the data through Alice's private key.[84] Bob is thus assured that the "Alice" who wants to transact with him is the same user "Alice" whom Bob can verify on the open ledger has the data to transact, and he can confidently transact back.[85] Even more important, Bob is also assured that no one tampered with the data Alice sent en route, even by one character—or else running the data through Alice's public key would have created a vastly different digest from Alice's signature digest.[86] The probability of error or breach is infinitesimally minute. "Asymmetric-key cryptography," therefore, "enables a trust relationship between users who do not know or trust one another, by providing a mechanism to verify the integrity and authenticity of transactions while at the same time allowing transactions to remain public."[87]

D. *Distribution and Openness*

Now let's move from the underlying technologies to their structural effects, and show how blockchain uses the technologies to dispense with intermediaries and secrecy without having to sacrifice security (and thus to understand why some see blockchain as promising a wholly new model in direct, frictionless human interactions). Notice that a moment ago Bob had to be able to check something: whether "Alice" had the data—the coin—she promised. How can he do that? Normally, a bank or central authority would do that work for Bob using its own books. Blockchain offers something else: a distributed, transparent ledger, a way for many computers ("nodes") in a network to share and store the same data at the same time, updating and reconciling the data together.[88] Each node has

[84] YAGA ET AL., *supra* note 3, at 11.

[85] *See* Nielsen, *Bitcoin Protocol*, *supra* note 28. Who the real-world person "Alice" actually is, of course, a separate issue.

[86] As with a hash, the slightest change to the underlying text creates a vastly different digest output. DE FILIPPI & WRIGHT, *supra* note 5, at 16.

[87] YAGA ET AL., *supra* note 3, at 11.

[88] ACT-IAC, ENABLING BLOCKCHAIN INNOVATION, *supra* note 6, at 4.

access to the entire chain and its complete history.[89] No single party controls or stores the data or acts as the central point of reconciliation.[90] But neither can any party unilaterally manipulate the data. These features create the fundamental shift in social relations and expectations that blockchain portends. In the physical world, obscurity, P2P trust, and third-party intermediaries are the *means* to achieve the *ends* of security, control, and antidotes to untrustworthy people, permitting us to direct our activities (reasonably) freely and without fear. On a blockchain, by contrast, *large-scale distribution* and *openness* are the means to achieve those same ends.

Broadly speaking, blockchains come in two types, characterized by their levels of distribution and openness.[91] The first type is the "permissionless" blockchain network, in which there is no central authority at all, and anyone can join and share data as they please.[92] Permissionless blockchains are also "open," meaning that the ledger data are visible to anyone who downloads the software and receives updates. The vast majority of current cryptocurrencies, as well as Ethereum (the second-most famous protocol after Bitcoin and a highly flexible blockchain that can power multiple use cases through distributed applications),[93] operate on open, permissionless blockchains.[94] The second type is the "permissioned" blockchain, in which an administrator decides which nodes can join the network, which can be "open" to the public or only to nodes with the

[89] Generally speaking. WERBACH, BLOCKCHAIN, *supra* note 2, at 83 (noting "light" users, who spare computer power by not publishing blocks, and who can access the full chain history but don't store it).

[90] *Id.* at 237.

[91] YAGA ET AL., *supra* note 3, at v; Suyash Gupta & Mohammed Sodoghi, *Blockchain Transaction Processing*, ENCYCLOPEDIA OF BIG DATA TECHNOLOGIES 4 (2018).

[92] YAGA ET AL., *supra* note 3, at 5; Hector Joseph Smith, Technical Analysis of the Bitcoin Cryptocurrency 68-69 (Apr. 12, 2015) (unpublished Bachelor Thesis, Hamburg Univ. Applied Sci.), https://perma.cc/7R9P-66P5 (describing how Bitcoin nodes power up and search out other nodes with which to synchronize a current copy of the ledger). On many permissionless blockchains, the software developers and major node operators may occasionally make fixes or adjustments to the protocol. But that does not mean that they ultimately control the data. YAGA ET AL., *supra* note 3, at 35.

[93] *See generally* Deborah Ginsberg, The Building Blocks of the Blockchain, 20 N.C.J.L. & TECH. 471, 484 (2019); Gavin Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger (2014) (unpublished manuscript), https://perma.cc/KA79-HD7F.

[94] Houben & Snyers, *supra* note 13, at 15. Note, however, that there are numerous gradations of openness among "open" chains. Some cryptocurrency protocols, for instance, such as Bitcoin, leave all transactions visible, while others, such as Monero, ZCash, and Dash offer more privacy protections than Bitcoin, obscuring in their public ledgers details such as addresses and amounts spent in their chains. There are, however, some tradeoffs in tamper-resistance and anti-fraud protection in these currencies. ROCIC, BITCOIN AND CRYPTOCURRENCIES, *supra* note 13, at 7.

administrator's permission.[95] This is the architecture that large companies most often use to interact with suppliers, customers, or other partners—which means that permissioned blockchains may be the interface by which large conglomerates store information about "ordinary" people on blockchains. The permissionless network promises the more radical shift in social relations, while permissioned networks retain some of a traditional business model.[96] But both kinds of blockchains are still novel, and both present Fourth Amendment implications: both still distribute information with varying degrees of openness among multiple actors to increase data security, and both create voluminous permanent records.

How, precisely, do distribution and openness achieve the ends of security and free flow of information? In the first place, distribution protects data from loss, attack, or censorship: there are currently over nine thousand active full nodes worldwide holding copies of the ledger in the Bitcoin network, for instance,[97] and if a node becomes unavailable, the blockchain data persist among the other nodes.[98]

But distribution also works with hashing, public-private key cryptography, and digital signatures to serve an even more sophisticated and novel purpose: creating security through transparency. Here's how: when two parties on a blockchain network wish to transact data, they broadcast the proposed transaction, digital signatures, and other information about the transaction to all other nodes on the blockchain to be "validated."[99] This information waits with other proposed transactions in a pool until it is organized into "blocks" as it is reviewed by other, validator nodes for accuracy. A validator node reviews the open ledger's record of all previous transactions and the proposed transaction's inputs and outputs (which should square out with the visible transactions in

[95] WERBACH, BLOCKCHAIN, *supra* note 2, at 59. Permissioned blockchains are sometimes also called "private" or "consortium" blockchains. Houben & Snyers, *supra* note 13, at 15. Generally speaking, therefore, parties on a permissioned chain will know each other, even if they do not fully trust each other. Indeed, certain businesses may be required to know their counterparties on a permissioned chain under Know Your Customer ("KYC") and anti-money laundering ("AML") laws. Ashley Longman, *The Future of Blockchain: As Technology Spreads, It May Warrant More Privacy Protection for Information Stored with Blockchain*, 23 N.C. BANKING INST. 111, 120 (2019).

[96] Nakamoto, *supra* note 12; Aaron Hankin, *Here's How Much It Costs to Mine A Single Bitcoin in Your Country*, MARKETWATCH (May 11, 2018), https://perma.cc/45W6-X7H9. For the impassioned debate about the relative merits of permissioned versus non-permissioned chains, see WERBACH, BLOCKCHAIN, *supra* note 2, at 62. This article does not take a stance in the debate; it only notes that both architectures distribute information with varying degrees of openness among multiple parties, with Fourth Amendment implications.

[97] Addy Yeow, *Global Bitcoin Nodes Distribution*, BITNODES (Apr. 10, 2019), https://perma.cc/4YFX-WZW6.

[98] Hence part of censorship-resistance. See YAGA ET AL., *supra* note 3, at 3, 13-15.

[99] *Id.* at 9.

previous blocks) as well as the transactors' digital signatures (which proves that they are who they say they are and thus own what the ledger says they own).[100]

If the pieces check out, the validator node prepares to publish the transaction for the other nodes to accept onto the permanent ledger. But before it can do so, it must take on some sort of cost. In the Bitcoin protocol and other cryptocurrencies, the cost is working out a complex cryptographical puzzle that is very computationally taxing in energy and time to solve, but easy for others to verify has been solved correctly.[101] This is called "proof of work."[102] Other blockchain protocols require a validator node to "stake" some cryptocurrency in exchange for the chance to publish a block, called "proof of stake."[103] Either way, a validator node must absorb this cost before it adds to the chain. The rest of the network then decides to approve or disapprove the addition based on the accuracy of the information proposed and the validator's proof. If the network approves, the validator node gets a reward, perhaps a newly "mined" coin.[104] If the network disapproves, the validator node gets no reward, and so has lost immense time and energy for no purpose, while the proposing nodes' transaction is also rejected. Every node is thus incentivized to propose and validate only blocks of accurate data to avoid squandering its own time and resources to no reward.[105] This open, distributed validation process obviates the need for a central third party to reconcile the ledger.

What happens next is the most sophisticated part of the technological discussion, but it is essential to understanding how openness and distribution actually create blockchain security. Each block has two parts: the data stored within the block (sometimes called the "payload")[106]—which could be any data

[100] Much of this process is automated by software. *Id.* at 18.

[101] YAGA ET AL., supra note 3 at 19-20; Nakamoto, *supra* note 12, at 3. Simplified, the puzzle in the Bitcoin protocol is for the validator node to find an integer (known as the "nonce") that, when hashed together with certain of the block's data, creates a digest with certain characteristics. The process is so computationally draining that it can use more electricity than used by some whole nations. Hankin, *supra* note 96.

[102] Commonly abbreviated "PoW." YAGA ET AL., *supra* note 3, at 17. For the technical details, see generally Gupta & Sodoghi, *supra* note 91.

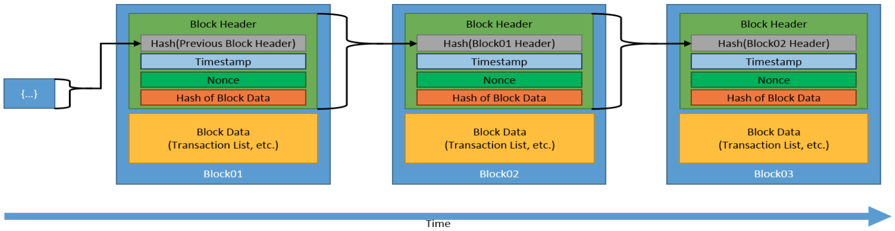
[103] Commonly abbreviated "PoS." WERBACH, BLOCKCHAIN, *supra* note 2, at 57. There are less common alternate proof methods, with various advantages and disadvantages and levels of centralization, but all with the purpose of making it more costly to cheat a blockchain than to support it. Giang-Truong Nguyen & Kyungbaek Kim, *A Survey About Consensus Algorithms Used in Blockchain*, 14 J. INFO. PROCESSING SYS. 101, 115-23 (2018).

[104] Andrew LR & Douglas A. Orr, *Bitcoin Investigations: Evolving Methodologies and Case Studies*, 9 J. FORENSIC RESEARCH 1, 2 (2018).

[105] *See* WERBACH, BLOCKCHAIN, *supra* note 2, at 100-01. Economists have modeled blockchain incentive mechanisms and found them generally sound, although usually with some suggestions for achieving greater efficiency. See, e.g., Bruno Biais et al., *The Blockchain Folk Theorem*, TOULOUSE SCH. ECON. 71, 38-39 (2018).

[106] Smith, *supra* note 92, at 55.

whatsoever—and the "header," a hash digest that identifies the block.[107] The header contains the result of hashing the data in the payload, the sender's public key and digital signature, and other data such as a time stamp and the header digest of the *previous* block on the chain.[108] The header of the previous block was similarly created by hashing its block's payload data and the header of *its* predecessor, and so on backwards. A block's header digest is thus rooted mathematically in every block of data that came before it, and then roots the header digest of every block that comes after it. Once the validator node publishes the proposed block, header, and proof, other nodes can "accept" the block by choosing to hash the next proposed block on top of it and sending update notices so that every node can join the "shared state" of the ledger.[109] Hence, the network collectively builds a "chain" of blocks mathematically connected by hash digests in their headers, and the total content of the blocks is the shared, open ledger of transactions:[110]



The upshot is that once block joins a chain, any subsequent change to the data within that block, *even a single bit or character*, would automatically algorithmically change its header digest radically.[111] That change would then transfigure the next block's header—rooted as it is in its predecessor's header hash—and so on down the line.[112] Therefore, to disguise a post-hoc change to a block—perhaps to erase the record of spending a cryptocoin so one could fraudulently spend it again later—a forger would have to re-hash it and then re-publish the next block in the chain with a new header, and then the next, and so on, for all the following blocks.[113]

[107] Bacon et al., *supra* note 26, at 19.

[108] Because the data on blockchains accumulate over time, there exist computational methods, beyond the scope of this paper, to streamline storage while maintaining immutability and visibility. *See, e.g.*, Nakamoto, *supra* note 12 (noting such solutions as a Merkle tree).

[109] De Filippi & Wright, *supra* note 5, at 24-25.

[110] Image from Yaga et al., *supra* note 3, at 17.

[111] *Id.*

[112] *Id.*

[113] *Id.*

Every node viewing the public copy of the chain would observe and reject this chicanery.[114] Distribution and openness thus make blockchain "tamper evident." More so, distribution and openness make the chain "tamper resistant": the *only* way to alter and re-publish a block is to "revalidate" and republish all the blocks and their headers in sequence from the fraudulent block up to the present.[115] That would require phenomenal (and ever-increasing) amounts of proof of work or proof of stake as the chain lengthens—all to no avail once any change is detected and rejected by the network of nodes anyway.[116] Attackers might try to get away with fraud by amassing 51% of the computing power of the network so that they could self-validate any transaction and repeatedly hash on top of it no matter who objected.[117] But that feat becomes inordinately difficult and costly once a distributed network gets large enough.[118]

Blockchain data records are hence (for all intents and purposes) "immutable" and irreversible.[119] Mathematics work with visible, distributed storage to protect data security, and drastically reduce the costs and uncertainty of relying on centralized third parties to combat fraud and hacking.[120] Distribution and

[114] *Id.* Rejected blocks are ignored and not built upon; the longest chain of blocks thus becomes the architecturally visible consensus of the network, plain to all, an agreed "state of information." Hurich, *supra* note 11, at 577.

[115] Bacon et al., *supra* note 26, at 17.

[116] Nielsen, *Bitcoin Protocol*, *supra* note 28 ("[D]ouble spending will be immediately spotted by other people on the [network] and rejected, . . . [a]nd unless [the thief] is able to solve the proof-of-work at least as fast as everyone else in the network combined—roughly, that means controlling more than fifty percent of the computing power—then she will just keep falling further and further behind [the consensus fork].").

[117] *Id.* Some blockchains also "lock" the chain at certain points, preventing any tampering before that point. YAGA ET AL., *supra* note 3, at 28. Moreover, blockchain enthusiasts are on the lookout for collusive behavior and trying to develop technologies to prevent it. *See, e.g.*, Muhammad Saad et al., *Exploring the Attack Surface of Blockchain: A Systematic Overview*, 30 (ARXIV No. 1904.03487v1 2019).

[118] Several hundred of the world's fastest supercomputers *combined* could not manage it in the Bitcoin network. Werbach, *Trust, but Verify*, *supra* note 4. In addition, as of October 2017 it would require around $937 million in electricity to take 51% control of the Bitcoin network. Frank Hofmann et al., *The Immutability Concept of Blockchains and Benefits of Early Standardization*, 2017 ITU KALEIDOSCOPE 1, 186 (Nov. 2017).

[119] There is proper disagreement with the commonly-used term "immutable." Blockchains can be changed; for example, by a 51% attack, or (with the consensus of the community) to repair damage or alter the protocol. Gideon Greenspan, *The Blockchain Immutability Myth*, MULTICHAIN (May 4, 2017), https://perma.cc/RXW7-A4GK. Such attacks have indeed happened. Werbach, *Trust, but Verify*, *supra* note 4; Saad et al., *supra* note 117, at 1. These instances, however, are rare, and their existence does not negate the overall point that blockchain users seek and reasonably expect security and (practical) immutability. *See* Ferguson, *IoT*, *supra* note 5, at 869 ("Even if sophisticated hackers could thwart [digital] security measures, a symbolic statement of security exists. After all, just because burglars and police can enter locked houses, it does not mean citizens lose a claim of security behind those walls.").

[120] Nakamoto, *supra* note 12, at 1.

openness—"structured transparency," as opposed to obscurity—are directly instrumental to desired ends of security and ease of information exchange, all without the downsides of total secrecy or P2P or Leviathan trust.[121]

In sum, blockchain takes the physical world drawbacks of a crowd of untrustworthy strangers and turns them into strengths: a group (the larger the better so that no one can control the majority of computing power), of selfish (and thus incentivized) strangers, checking in on each other's (publicly available) data, all using hash functions to verify a transaction's accuracy and each other's work. Openness and broad distribution create the ends that obscurity-as-security, P2P trust, and Leviathan trust once vindicated in the physical world.[122]

E. Security and Pseudonymity

To be sure, not all aspects of a blockchain are fully transparent for all the world (including, as it happens, law enforcement) to see. Blockchain users are usually represented by one or more cryptographic addresses.[123] The address is public, but is also a creature of cryptography: to create an address in the Bitcoin protocol, for instance, the user takes a random 256-digit number and runs it through his or her public key algorithm and several hash algorithms to generate an address chain of a set number of characters.[124] Through hashing, the address cannot be directly connected to the user's public or private key. Indeed, on many blockchains, the ledgers are open and the only things kept entirely private are the real-world identities of the node users and transactors, the transactions occurring only between addresses using private key signatures to verify the transactions.

There is, however, a tension between privacy and openness on blockchains, and public blockchain users always take some risk of their activities being traced to them.[125] Commercial cryptocurrency exchange platforms—which act as marketplaces to trade tokens for each other or into traditional cash—for instance,

[121] WERBACH, BLOCKCHAIN, *supra* note 2, at 106.

[122] Andreas Antonopoulos, *Bitcoin Security Model: Trust by Computation*, O'REILLY RADAR (Feb. 20, 2014), https://perma.cc/MC7V-PFBZ ("Bitcoin fundamentally inverts the trust mechanism of a distributed system. Traditionally . . . trust is achieved through access control, by carefully vetting participants and excluding bad actors. . . . By contrast, bitcoin implements a trust model of trust by computation. . . . [T]he most important effect of this new trust model of trust-by-computation [is that] no one actor is trusted, and no one needs to be trusted.").

[123] YAGA ET AL., *supra* note 3, at 12.

[124] An example of an address in the Bitcoin protocol is 1K31KZXjcochXpRhjH9g5MxFFTHPi2zEXb. Ameer Rosic, *Blockchain Address 101: What Are Addresses on Blockchains?*, BLOCKGEEKS, https://perma.cc/8EJK-42FC (archived Oct. 4, 2019).

[125] Blockchain users must take care what visible data they post onto the network, and it may be wise to store some sensitive information "off-chain," with only hash digests of data kept "on-chain" to ensure the off-chain data are not tampered with. *See* ACT-IAC, ENABLING BLOCKCHAIN INNOVATION, *supra* note 6, at 7.

have cooperated with law enforcement to try to identify hackers and criminals using their systems.[126] Computer scientists, law enforcement, and specialized private network analysis companies such as Chainalysis and CoinSeer are also working together and are becoming more capable of connecting an anonymous address's pattern of activity and other indicia of blockchain network use to specific IP addresses, and thus to real-world users.[127]

Nevertheless—and of import to our Fourth Amendment analysis—these methods are at present specialized and intensive, requiring, for instance, harvesting network data from thousands of users for months on end through dummy "listening" nodes, and then subjecting the culled data to complex probability analyses.[128] There is also an arms race between network users and network observers for technologies that can "tumble" and mix transactions and addresses to obscure traces of and patterns in blockchain activities.[129] Cryptocurrency users, for instance, often create and use multiple addresses to help obfuscate their activities,[130] and cryptocurrencies such as Monero and ZCash tout powerful anonymity protections.[131] In all, a sophisticated blockchain user can reasonably expect not to be identified absent highly intricate efforts by an unusually sophisticated attacker or spy,[132] and a well-built blockchain "system can still provide significant privacy-guarantees while making the process of state

[126] *See, e.g.*, Joseph Young, *ShapeShift Is Assisting Police To Trace Cashed Out Bitcoin From WannaCry Ransomware*, CNN (Aug. 10, 2017), https://perma.cc/7MYF-E8PV.

[127] Jamie Redman, *U.S. Law Enforcement Wants Blockchain Surveillance Tools for Privacy Coins*, BITCOIN NEWS (Dec. 3, 2018), https://perma.cc/94F7-ZHE4.

[128] LR & Orr, *supra* note 104, at 6 (noting that a "wide net must be cast, *comprising of all active Bitcoin clients*, to glean information that can lead to a connection between a bitcoin address and an IP address") (emphasis added); Péter L. Juhász et al., *A Bayesian Approach To Identify Bitcoin Users*, 13 PLOS ONE e0207000 (2018).

[129] *See, e.g.*, Jordan Clifford, *Privacy On the Blockchain*, HACKERNOON (Oct. 5, 2017), https://perma.cc/D3Y7-55C6; Thibault de Balthasar & Julio Hernandez-Castro, *An Analysis of Bitcoin Laundry Services*, 22D NORDIC CONF. ON SECURE IT SYS. (2017).

[130] Clifford, *supra* note 129.

[131] *See supra*, note 110. The government is currently looking for a way to trace these currencies. Jamie Redman, *US Law Enforcement Wants Blockchain Surveillance Tools for Privacy Coins*, BITCOIN NEWS (Dec. 4, 2018), https://perma.cc/29H5-RJ7J.

[132] LR & Orr, *supra* note 104 ("Overall, the quest for privacy in Bitcoin transactions, especially by sophisticated users, is meeting with success."). *But see id.* ("Peer-to-peer network analysis has met with some success in linking transactions to IP addresses, but requires a long-term, live connection to the Bitcoin network, or the results of a previous connection from software such as CoinSeer. . . . Unless you are very careful in the way you use Bitcoin [and you have the technical know-how to use it with other anonymizing technologies like Tor or i2p], you should assume that a persistent, motivated attacker will be able to associate your IP address with your bitcoin transactions."); *but see* (again) Ferguson, *IoT*, *supra* note 5 ("Even if sophisticated hackers could thwart [digital] security measures, a symbolic statement of security exists. After all, just because burglars and police can enter locked houses, it does not mean citizens lose a claim of security behind those walls.").

transitions transparent, e.g. a distributed ledger can provide public verifiability of its overall state without leaking information about the state of each individual participant."[133]

* * *

Let's sum up so far. Blockchain does not simply translate antidotes for an untrustworthy physical world into digital analogies. Instead, it turns physical means to security and freedom of activity on their heads, or completely reimagines them. Blockchain adopts obscurity-as-security, but only in part: it deeply cloaks computer operators' true identities but often makes all else public and visible, with the radical insight that in the right digital circumstances, things openly shared and seen can be more secure from censorship and damage than things hidden. Blockchain does not create a digital analogy to lost P2P trust by attempting, say, to re-create a digital "community" of trusted acquaintances: it simply obviates the loss of trust by making it mathematically intractable for untrustworthy actors to manipulate others' data no matter how much they would like to. And it (largely) abandons Leviathan intermediaries and reassigns their roles to scattered network participants, with the further radical insight that in the right digital circumstances a crowd of strangers can keep information more secure than can an individual third-party gatekeeper. In short, it envisions a new set of social norms and uses new technological methods to achieve fundamental and ancient human desires.

These kinds of conceptual inversions and transpositions should make us cautious when we cross from legal doctrine created for the physical world to consider how Fourth Amendment doctrine and blockchain will interact. And because blockchain is a technology imbued in political and social theory about privacy, property rights, centralized authority, and human autonomy, it offers a rich challenge for Fourth Amendment doctrine, which addresses many of the same concerns, and to which we now turn.

III. BLOCKCHAIN AND THE FOURTH AMENDMENT

A. *Doctrine:* Boyd *to* Katz

Fourth Amendment doctrine has shifted focus repeatedly during its development, especially in the face of developing technologies. Federal courts paid little attention to the Amendment until 1886 in *Boyd v. United States*, a civil forfeiture dispute in which a district court ordered a government supplier to turn over its invoices.[134] The Supreme Court reversed, using astoundingly far-reaching rhetoric that decried any invasion of "the sanctity of a man's home and the

[133] Wüst & Gervais, *supra* note 15.

[134] Boyd v. United States, 116 U.S. 616 (1886).

privacies of life"—though Boyd's home had no role in the case—"the invasion of his indefeasible right of personal security, personal liberty, and private property," and "any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods."[135] *Boyd*'s laissez-faire constitutionalism would wrap all manner of commercial and personal activities and property, no matter where situated, in Fourth Amendment protection.[136]

Boyd proved unduly constricting to criminal enforcement.[137] During Prohibition, the Court narrowed *Boyd* and its "extreme" progeny in *Olmstead v. United States*,[138] holding that the Fourth Amendment did not cover tapped phone conversations: only "material things," not intangible conversations, were within the Amendment's "persons, houses, papers, and effects," and, on top of that, no "entry" was made onto the defendant's property.[139] This highly literalist,[140] property-focused approach sparked impassioned dissents and appeal to *Boyd*'s civil libertarianism in the face of new and invasive technologies.[141]

Olmstead's hyper-technicality, however, also proved untenable, and was rejected in *Katz v. United States*, which arose from a probe into a gambling ring during which investigators eavesdropped on the defendant's telephone conversations using a device placed on a public telephone booth.[142] The Court overturned *Olmstead*'s narrow analysis, famously holding that the Fourth Amendment protects "people, not places."[143] The crux of the majority opinion was that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protections," but "what he seeks to preserve as private, even in an area accessible to the public, may be

[135] *Id.* at 630.

[136] *See* Richard A. Epstein, Entick v. Carrington *and* Boyd v. United States*: Keeping the Fourth and Fifth Amendments on Track*, 82 U. CHICAGO L. REV. 27, 39 (2015).

[137] William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393 (1995) [hereinafter Stuntz, *Substantive Origins*].

[138] 277 U.S. 438, 463 (1927).

[139] *Id.* at 430.

[140] Morgan Cloud, *The Fourth Amendment during the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 555,631 (1996) [hereinafter Cloud, *Privacy, Property, and Liberty*].

[141] We will return to Justice Brandeis' famous dissent below in Part III.D.3. The Court nevertheless doubled down on the "trespass rule" in *Goldman v. United States*, 316 U.S. 129, 131-32 (1942) (holding no physical trespass and thus no search when federal agents amplified sound from a room adjoining defendant's); and *Silverman v. United States*, 365 U.S. 505, 506, 512 (1961) (holding spike mike that intruded a "fraction of an inch" into defendant's property triggered Fourth Amendment).

[142] Katz v. United States, 389 U.S. 347, 348 (1967).

[143] *Id.* at 351.

constitutionally protected."[144] Justice Harlan filled out the majority's statement in his concurrence, requiring a two-step test: "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.'" He continued: "Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."[145] The test in its currently operative formulation holds that "when an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable," "official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause."[146]

To summarize roughly, as the physical records in *Boyd* gave way to the intangible telephone conversations and wiretapping devices of *Olmstead* and *Katz*, the Court's Fourth Amendment focus changed from general security from government intrusion into one's papers and personal and business affairs[147] to a narrower focus on private property,[148] then to its current "lodestar,"[149] solicitude for "privacy," which was apparently assumed to cover any and all Fourth Amendment concerns. Larger constitutional processes, to be sure, underlay that arc,[150] but societal changes and advances in technology catalyzed those shifts.[151]

Future shifts, then, should be expected as technology further advances and society changes with it—especially because with those advances the *Katz* test has

[144] *Id.*

[145] *Id.* at 361 (Harlan, J., concurring).

[146] *Carpenter*, 138 S. Ct. at 2213 (2018) (internal quotations and citations omitted).

[147] Thomas Y. Davies, *Can You Handle the Truth? The Framers Preserved Common-Law Criminal Arrest and Search Rules in "Due Process of Law"—"Fourth Amendment Reasonableness" Is Only a Modern, Destructive, Judicial Myth*, 43 TEX. TECH. L. REV. 51, 117 (2011) [hereinafter Davies, *Can You Handle the Truth?*] (seeing *Boyd* as "in keeping with [the Court's] campaign to protect business interests from government regulation").

[148] *But see* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67 (2013) (arguing that the Court did not strictly conceive of the test as a "trespass" or property test).

[149] Smith v. Maryland, 442 U.S. 735, 739 (1979).

[150] *See, e.g.*, AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 22 (1997); Stuntz, *Substantive Origins*, *supra* note 137, at 428-33 (showing how the Court collapsed *Boyd* as part of its making peace with the anti-Lochnerian regulatory state).

[151] *See* Katherine Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 628 (2011) ("*Katz* was not about the evolution of invasive technological means to penetrate traditionally private spaces. Rather, it was about the ways in which technology-mediated social change had exposed the citizenry to intrusive surveillance."); Neil Richards, *The Third Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1447-65 (2017) (describing how Fourth Amendment law tends to "lag" behind advancing technologies that eventually force updates to doctrine).

become subject to biting criticism.[152] It has been called an "embarrassment,"[153] "circular, indeterminate, and self-validating,"[154] a "failed experiment,"[155] and "notoriously unhelpful" and "self-indulgent."[156] Disapproval of the test crosses political lines.[157]

There are generally three (somewhat overlapping) criticisms of the test.[158] First, that "privacy" is an imprecise and unstable concept upon which to rest a fundamental constitutional right.[159] "Privacy" is "notoriously difficult to define,"[160] and may shift meanings erratically as cultural norms change.[161] That imprecision, critics fear, has led to "inconsistent and bizarre" results,[162] which actually undercut society's privacy long-term.[163] In particular, attempts to cram newer and ever-

[152] *See, e.g.*, *Carpenter*, 138 S. Ct. at 2244, n.10 (2018) (Thomas, J., dissenting) (collecting critiques); Cloud, *Privacy, Property, and Liberty*, *supra* note 140, at 555, n.1 (same); Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security*, 33 WAKE FOREST L. REV. 307, 339 n. 234 (1998) [hereinafter Clancy, *Property, Privacy, or Security*] (same); Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?*, 94 COLUM. L. REV. 1751 (1994) (same).

[153] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757 (1994).

[154] *See, e.g.*, Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 105-9 (2010) (arguing that the test purportedly relies on society's expectations of privacy to formulate its rules while also setting society's expectations of how police will act in response to its rules). *But see* Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHICAGO L. REV. 1747 (2017) (finding little empirical support for the claim of circularity).

[155] *Carpenter*, 138 S. Ct. at 2246 (Thomas J., dissenting).

[156] Minnesota v. Carter, 525 U.S. 83 (1998).

[157] Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L. J. 19, 20-21 (1989) (noting the "virtual unanimity, transcending normal ideological dispute, that the Court simply has made a mess of search and seizure law").

[158] Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH. L. REV. 143, 145 (2015) [hereinafter Slobogin, *A Defense of Privacy*].

[159] *Id.* at 148-49.

[160] Wasserstrom & Seidman, *supra* note 157, at 59-60 (gathering competing definitions of privacy); Anna Lvovsky, *Fourth Amendment Moralism*, 166 U. PA. L. REV. 1189, 1244 & n.321 (2018); James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 662-63 n.76-78 (1985).

[161] Lvovsky, *supra* note 160, at 1194.

[162] Wasserstrom & Seidman, *supra* note 157, at 29; *see also* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) ("The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence."); Slobogin, *A Defense of Privacy*, *supra* note 158 at 149 (arguing same, collecting cases).

[163] *See, e.g.*, John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WIS. L. REV. 655, 665 (2008).

more probing technologies (helicopters,[164] beepers,[165] heat-readers[166]) into the reasonable expectation of privacy framework have left a morass of contradictions and confusion.[167]

Worse, the criticism goes, to the extent that the Court has settled on a definition of privacy, it has decided that "privacy" means *only* keeping activities in total "secrecy" from others—what William Stuntz once termed "privacy-as-secrecy"—an unreasonable expectation in modern life that drastically cabins possible Fourth Amendment claims.[168] Many worry that as technology becomes even more pervasive and invasive—think facial recognition software,[169] drones,[170] constant data collection from our myriad devices[171]—and as privacy-as-secrecy becomes ever more impossible, the *Katz* test will turn the Fourth Amendment into a "dead letter."[172]

The second criticism is that *Katz* improperly substituted "privacy" as a flawed proxy for some truer purpose of the Fourth Amendment, and that doctrine should shift again, away from the proxy and towards the fundamental Fourth Amendment principle or principles that "privacy" only imperfectly upholds.[173]

[164] Florida v. Riley, 488 U.S. 445 (1989).

[165] United States v. Knotts, 460 U.S. 276 (1983).

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

[167] Richards, *supra* note 151, at 1464-65; Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 264 (2016) (arguing that applying *Katz* to multifarious technologies has led to "incongruous decisions").

[168] .William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1023 (1995) [hereinafter Stuntz, *Privacy's Problem*]; DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 99-101, 110, 177 (2011) (arguing that privacy-as-secrecy constricts Fourth Amendment protections); Sundby, *supra* note 152, at 1763 (arguing the same, especially as technology becomes more pervasive).

[169] *See, e.g.*, Elizabeth Snyder, *"Faceprints" and the Fourth Amendment: How the FBI Uses Facial Recognition Technology To Conduct Unlawful Seaches*, 68 SYRACUSE L. REV. 255, 257 (2018).

[170] *See, e.g.*, Matthew R. Koerner, *Drones and the Fourth Amendment: Redefining Expectations of Privacy*, 64 DUKE L.J. 1129 (2015).

[171] *See, e.g.*, Donohue, *supra* note 24, at 554 ("Digital information is ubiquitous. Individuals cannot go about their daily lives without generating a footprint of nearly everything they do. The resulting data is accessible, recordable, and analyzable."); Gabriel R. Schlabach, *Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677, 687-90 (2015) (describing data collection in common devices and apps).

[172] *See, e.g.*, Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1309, 1320 (2012); Rubenfeld, *supra* note 154, at 118 ("So long as Fourth Amendment privacy is parasitical on private-sphere privacy, the former must die as its host dies, and this host is undoubtedly faltering today in the networked, monitored and digitized world we are learning to call our own.").

[173] Ohm, *supra* note 172, at 1336 ("Privacy is simply a proxy for what the amendment protects. It is a proxy that served us well for a long time because technology and social practices have historically moved so slowly. . . . But the age of using privacy as a measuring stick for

Scholars have suggested several replacement candidates: human dignity,[174] mutual trust between government and citizen,[175] personal autonomy and self-definition,[176] refuge from society's pressures,[177] liberty to define interpersonal relationships,[178] free expression and association (especially in historical conjunction with the First Amendment),[179] and restraint of and security against government intrusion or coercion.[180] Having identified a candidate replacement value, the question usually becomes "whether the value said to underlie the Fourth Amendment is susceptible to principled application."[181]

The third criticism is that *Katz* simply ignored the Fourth Amendment's plain language.[182] The Amendment, of course, never mentions "privacy." Instead, it protects the "right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures."[183] *Katz*'s substitution of "privacy" for the Fourth Amendment's text, the critique continues, essentially turns the test into policymaking about how judges think "privacy" should operate,[184] or invites error-ridden guesses of how much or what kind of privacy

Fourth Amendment protection is likely soon to draw to a close."); Slobogin, *A Defense of Privacy*, *supra* note 158, at 151-56; Stuntz, *Privacy's Problem*, *supra* note 168, at 1023 ("[T]he Fourth Amendment must protect something besides privacy-as-secrecy."); Rubenfeld, *supra* note 154, at 115 ("The Fourth Amendment must cut anchor with the expectations-of-privacy apparatus").

[174] Castiglione, *supra* note 163.

[175] Sundby, *supra* note 152, at 1754-55.

[176] Lvovsky, *supra* note 160, at 1189; Tomkovicz, *supra* note 160, at 645, 662.

[177] David Alan Sklansky, *Too Much Information: How Not To Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1070, 1074, 1107-10, 1113 (2014) [hereinafter Sklansky, *Too Much Information*].

[178] Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After Lawrence*, 57 UCLA L. REV. 1, 59 (2009).

[179] *See generally* Price, *supra* note 167; SOLOVE, *supra* note 167, at 118-19.

[180] *See, e.g.*, Ohm, *supra* note 172 at 1312; Donohue, *supra* note 24 at 682. *See also* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602-1791, 770 (2009) (Fourth Amendment "expressed not a single idea but a family of ideas whose identity and dimensions developed in historical context").

[181] Slobogin, *A Defense of Privacy*, *supra* note 158, at 148.

[182] Justice Black, dissenting in *Katz*, was the first to object to "the 'broad, abstract and ambiguous concept' of 'privacy' as a 'comprehensive substitute for the Fourth Amendment's guarantee against 'unreasonable searches and seizures." *Katz*, 389 U.S. at 347 (Black, J. dissenting); *see also Carter*, 525 U.S. at 97 (1998) (the reasonable expectation of privacy test "has no plausible foundation in the text of the Fourth Amendment").

[183] U.S. CONST. amend. IV (emphasis added).

[184] *See, e.g.*, *Carter*, 525 U.S. at 97 ("In my view, the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, those 'actual [subjective] expectation[s] of privacy' 'that society is prepared to recognize as "reasonable,"' . . . bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable.") (Scalia, J., concurring) (quoting *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring)); *Carpenter*, 138 S. Ct. at

society expects,[185] all divorced from the Fourth Amendment's wording and history.

Blockchain significantly advances all three criticisms, and its novel openness and distribution compels us like no other current technology to engage and rethink common Fourth Amendment definitions, doctrines, and analogies that are rooted in the experience of physical space. Blockchain can fit, in part, within the current doctrinal framework of privacy-as-secrecy in keeping its users' identities cryptographically shrouded and its private keys hidden. But its openness and distribution gravely challenge the rest of the current framework. Blockchain exemplifies how "privacy" can shift meanings as technology shifts, and how privacy can connote both secrecy and also control of information and identity—even in public. More important, blockchain advances several ends that the Fourth Amendment might comprehend—including security from Leviathan intrusion, free expression, and personal autonomy—by *abandoning*, not relying on, privacy-as-secrecy. And, ironically enough, the twenty-first century's latest technology shows how the eighteenth century text's focus on ownership and control may be a better means to achieve fundamental human ends than privacy-as-secrecy.

B. Blockchain and Katz*: A Bare Fit*

How does blockchain fit into doctrine as it currently stands, with its particular focus on privacy-as-secrecy? In what hidden things, if anything, do blockchain users have a "reasonable expectation of privacy," an invasion of which would generally require a warrant?[186]

First, there is a reasonable expectation of privacy in the private key, which is unlikely to be exposed to anyone. Proven possession of the key, of course, could connect individuals to their blockchain activities, and thus would be of interest to law enforcement. As noted, the private key can be stored in a person's computer

2265 (Gorsuch, J., dissenting) (arguing that the *Katz* test "often calls for a pure policy choice"); Wasserstrom & Seidman, supra note 157 at 50 ("[It is] embarrassingly obvious that the Court is not reasoning disinterestedly from obvious first principles. Instead, its resolution of the search and seizure problem rests on controversial value choices.").

[185] *See, e.g.*, Henry F. Fradella et al., *Quantifying* Katz*: Empirically Measuring Reasonable Expectations of Privacy in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 381 (2011) (showing results of empirical studies of the public's reasonable expectations of privacy, which markedly differed from judicial assessments); Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 58 (2015) (same); Bernard Chao et al., *Why Courts Fail To Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263 (2018) (explaining how judges' biases can affect assessments of reasonable expectations of privacy).

[186] *Carpenter*, 138 S. Ct. at 2213.

or device, but can be stored offline, even on physical paper.[187] Courts generally treat computer drives and devices as private containers subject to a warrant requirement.[188] If a sought key is stored there, or stored physically in a person's home or office, the Fourth Amendment analysis would be simple: the police should get a warrant for it. Indeed, the Justice Department's model electronic-evidence warrant includes encryption keys in its sample list of target items to be seized from a computer.[189]

The picture is only slightly more complicated if the key is stored in a password-protected "wallet." Wallets, recall, are commercially available computer programs that are often used to store keys and keep accounts of cryptocurrency transactions. The storage function and perhaps the very name "wallet" have encouraged courts to analogize the wallet to a file or container, particularly if law enforcement accesses the wallet by first physically seizing the defendant's computer.[190] Now, it might be said that the key has been "shared" with a commercial wallet company, as with a bank account. That precise issue has not yet apparently been litigated, but may turn on the extent to which the wallet company can access the wallet data.[191] We will return to the third-party doctrine below, but given the analogy, a password-protected wallet whose data are not shared with or reasonably accessible to others should enjoy a reasonable expectation of privacy.

Another thing in which blockchain users may have a reasonable expectation of privacy-as-secrecy is their identity, represented digitally by their address(es). An address string, of course, is public, and would retain no reasonable expectation of privacy under current doctrine, especially if a person has publicly connected

[187] *See supra*, note 95.

[188] Yale Kamisar & J.H. Israel, *Wayne R. LaFave: Search and Seizure Commentator at Work and Play*, U. ILL. L. REV. 187 (1993); Riana Pfefferkorn, *Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?*, 49 CONN. L. REV. 1393, 1440 & n.297 (2017) (collecting cases).

[189] Pfefferkorn, *supra* note 188, at 1432-33 (citing OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATTORNEYS, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 249 (2009)) .

[190] *See, e.g.*, United States v. 50.44 Bitcoins, No. ELH-15-3692, 2016 WL 3049166, at *2 (D. Md. May 31, 2016); United States v. Ulbricht, 858 F.3d 71, 85 n.7 (2nd Cir. 2017).

[191] Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 906-08 (9th Cir. 2008) (finding reasonable expectation of privacy in pager messages based on an "informal policy" of the provider "that the text messages would not be audited," but noting "this is necessarily a context-sensitive inquiry"), *rev'd on other grounds by* City of Ontario v. Quon, 560 U.S. 746 (2010)). Part of the question would also rest on whether the Stored Communications Act (SCA) applied to the specific wallet, e.g., whether the "wallet" was remote storage or was merely a computer program on an individual's computer. *See How To Store Your Bitcoin*, COINDESK, https://perma.cc/928C-D8S8 (archived Dec. 28, 2019). On the implications of the SCA on blockchain, see *infra* note 248.

their true identity to it.[192] Addresses are also often stored in wallets, and hosted wallet companies are required to comply with know-your-customer and anti-money-laundering laws,[193] obtaining customers' records and true identities, which the government might duly seek via subpoena.[194]

But what about users who do not use commercial wallet services, or who otherwise do not reveal their identities to third parties? That is, is there any reasonable expectation of privacy in the hidden underlying *identity* of the user if the user has not voluntarily relinquished it?

Many years ago, Alan Westin argued that a "state of privacy . . . occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance."[195] More recently, Jeffrey Skopek has shown that privacy is only half of an equation: "Privacy involves hiding the *information*, whereas anonymity involves hiding what makes it *personal*."[196] In other words, "we should not define anonymity as the condition of being *unidentifiable* . . . but rather as the condition of being *unidentified* at a given time and place."[197] Skopek identifies structural features of the world (large crowds, complex street grids) that dissociate a person's public actions from the person's identity, leading to a "reasonable expectation of anonymity" even in public.[198] In the digital space, he argues, the use of pseudonym is such a structural feature of anonymity.[199]

By this strong logic, blockchain users with digital addresses should reasonably expect privacy in their identities, even though they might operate in "public" on an open chain. To be sure, the growing knowledge that one might not be fully anonymous on a blockchain (as exemplified by the aforementioned anonymization "arms race")[200] might cut against an expectation of anonymity's

[192] See, e.g., Nielsen, *Bitcoin Protocol*, *supra* note 28, who provides his personal bitcoin address on his blog.

[193] Nikhilesh De, *FinCEN Says Some Dapps Are Subject to US Money Transmitter Rules*, COINDESK (May 9, 2019), https://perma.cc/YZ3C-FTB5.

[194] In 2018, for instance, the IRS forced Coinbase after more than a year of litigation to comply with a summons seeking taxpayer IDs, personally identifiable information, and records of account activity for thousands of accounts over a two-year period. United States v. Coinbase, Inc. (N.D. Cal. 2017). *But see* Caitlin Long, *Supreme Court and Digital Privacy: Should Blockchain Companies Challenge the Bank Secrecy Act?*, FORBES (Jun. 28, 2018), https://perma.cc/YFU8-LB5Q (arguing that the Coinbase result might have been different and users' identities might have been protected after *Carpenter*).

[195] ALAN F. WESTIN & DANIEL J. SOLOVE, PRIVACY AND FREEDOM 7, 31 (2015).

[196] Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, 101 VA. L. REV. 691, 694 (2015).

[197] *Id.* at 725.

[198] *Id.*

[199] *Id.* at 757.

[200] *Supra*, note 128.

being reasonable in a given fact pattern. But the facts that de-anonymization is so very difficult and cryptography so very powerful cuts in the opposite direction.[201] De-anonymization is currently the purview of experts willing to spend months on data gathering and analysis. The process is reminiscent of *Kyllo v. United States*, the famed "thermal imager" case, in which the Court held that people retain a reasonable expectation of privacy in constitutionally protected spaces against intrusive technologies "not in general public use."[202]

Moreover, while the Supreme Court has never defined public anonymity as being within "privacy" in so many words, there have been robust hints.[203] *Katz* itself noted that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all," and cited as examples goods seized openly or the embarrassment of public arrest.[204] Most recently, in *Carpenter v. United States*, which we will discuss in detail, the Court reiterated that there is a reasonable expectation of privacy in the "whole of [one's] physical movements," even when the physical movements are tracked through commercial records created by third parties.[205] Applying this and Skopek's logic, a user's anonymity, under pseudonymous address, and particularly if tumbled for use even in public activities on a blockchain, should receive some level of Fourth Amendment protection.[206]

In all, the private key, the wallet, and a blockchain user's identity can fit either under the current framework of privacy-as-secrecy or under a slightly expanded view of *Katz* as encompassing privacy-as-anonymity. That might be enough

[201] Orin Kerr has argued that cryptography cannot create a reasonable expectation of privacy, on grounds that it is like a language or a lock and key, which one can reasonably expect others to discover. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?*, 33 CONN. L. REV. 503 (2001). These points and metaphors have been strongly rebutted, given the awesome power of modern cryptography. *See, e.g.*, David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2226 (2009); Sean J. Edgett, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, 30 PEPPERDINE L. REV. 339, 355-61 (2003); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 532 (2005).

[202] *Kyllo*, 533 U.S. at 40; Raymond Ku, *The Founders' Privacy: The Fourth Amendment and The Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1329 (2002) ("*Kyllo* suggests that government use of new technologies should always be subject to the warrant requirement unless they are in general public use.").

[203] Skopek, *supra* note 196, at 727-32 (analyzing cases).

[204] *Katz*, 389 U.S. at 350 n.4.

[205] *Carpenter*, 138 S. Ct. at 2219.

[206] *See* Donohue, *supra* note 24, at 679 ("[T]he collection of uniquely identifiable information, i.e., data that relates, and could be traced back, to unique individuals, may constitute a search per se, requiring a warrant for collection."); Ohm, *supra* note 172, at 1339 ("In the future, the police request alone will satisfy state action.").

analysis for some criminal investigations, especially those that seek merely to search a specific defendant's physical computer or files for data in that computer related to his blockchain activity. Not surprisingly, though, these are the aspects of blockchain that most easily analogize to obscurity-as-security in the physical world.

C. Blockchain's Challenge to "Privacy"

Now consider the effect of how blockchain's idiosyncratic combination of pseudonymity with openness and distribution shears away from easy physical analogy.

First, it warps the valences of "privacy," and thus advances the first criticism of *Katz*, that "privacy" is a vacillating concept. Privacy scholars have noted that "privacy" is "capacious," with multiple connotations.[207] Daniel Solove, for example, has identified at least six distinct ways to conceptualize "privacy": (1) the right to be let alone, (2) autonomy or the limited access to the self, (3) secrecy or concealment of discreditable information, (4) control over one's personal information, (5) personhood and preservation of one's dignity, and (6) intimacy and the promotion of relationships.[208] Compare these insights to a current claim about "privacy" on blockchain:

> In reality, one of the greatest benefits of the blockchain is that it makes it easy to achieve privacy without secrecy. When leveraged the right way, blockchain technology can protect private data without requiring murky, secretive operations.
>
> Put simply, secrecy means withholding information, even from people who have a legitimate right to access it because it affects them. Secrecy can be a harmful quality.
>
> In contrast, privacy refers to the ability of an individual to control the sharing of information that they rightfully own. Privacy is a right that we should all enjoy.[209]

You see the idea: privacy-as-secrecy is part of blockchain's definition of "privacy," but not its entire definition. Blockchain can also claim to vindicate

[207] *See, e.g.,* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1099-21 (2002); Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1048 (2018) (noting multiple definitions of privacy).

[208] Solove, *supra* note 207 at 1087, 1092, 1099-121.

[209] *Differentiating Between Privacy and Secrecy on the Blockchain*, BITCOIN MAGAZINE (Feb. 21, 2018), https://perma.cc/R9FQ-TQVF.

privacy-as-control-over-personal-information, privacy-as-autonomy, privacy-as-a-dignity-of-personhood.[210] It does so by abandoning *total* privacy-as-secrecy in favor of distribution and openness. Blockchain thus exposes the slippery and multifarious nature of "privacy," rejects one of its narrow definitions, and then concretizes different connotations of the concept into a novel technological architecture.

Moreover, blockchain forces us to consider that technology might make "privacy" so malleable that it might even encapsulate "public" acts. Consider an argument of Skopek, that

> Performing an action in public does not necessarily extinguish the privacy interests of the actor. As long as the action is anonymous, the disaggregation of the action and identity is maintained, thereby protecting the privacy of the actor. . . . In this way, a reasonable expectation of anonymity can support a reasonable expectation of privacy, thereby bringing anonymity interests (and public facts) into the scope of the "privacy" protections recognized by the Fourth Amendment.[211]

Blockchain's architecture uniquely reifies Skopek's insight that even *public actions* can be re-defined as "private" when the actor is anonymous. On a blockchain, openness and distribution are necessary instruments to reach the greater ends of control and security, while anonymity "disaggregates" the actors from the action, and thus from any discernable meaning or context to an outsider; a visible exchange of data might be a drug deal or a valid payment for a lawyer, but the observer cannot know, and the anonymous transactors do not care to share. Their action is thus public and yet, paradoxically, recognizably and meaningfully "private," all at once. But if privacy can be intertwined with publicity, then "privacy-as-secrecy" is no longer sufficient as a meaningful doctrinal category, and thus as a clear foundation for rights. Blockchain's unique combination of openness and pseudonymity exemplifies how chimerical constitutional protections can quickly become if they rest on "privacy."

D. *Fourth Amendment Values*

But blockchain does much more than just muddle definitions of a notoriously fraught term. More deeply, its idiosyncratic architecture upsets some of *Katz*'s foundational assumptions about society and human interaction.

[210] *See* Sklansky, *Too Much Information*, *supra* note 177, at 1102 ("[P]rivacy itself consists in something other than control over information, something at once more basic and potentially more expansive.").

[211] Skopek, *supra* note 196, at 726.

To see how, consider not just addresses and keys, but blockchain transaction data themselves—particularly data shared publicly on open chains—in light of the second criticism of *Katz*, that the Court substituted "privacy" as a proxy for or a means towards some truer ends of the Fourth Amendment. Blockchain is particularly relevant to three ends that critics have proposed: (1) security against government intrusion into citizens' lives, (2) the right to secure expression (especially in conjunction with the First Amendment), and (3) personal autonomy.[212] *Katz*'s privacy-as-secrecy is normally instrumental to these ends, and as such has become confused with them. But blockchain achieves those same ends through openness and distribution of its data. When that happens, *Katz*'s privacy-based framework ceases to be a useful analytical tool.

1. *Security from Government Intrusion*

The doctrinal proxy of privacy for security seems to have arisen from two suppositions from the Fourth Amendment's text. One, that a "search" must be for something that is hidden, hence private. Often true, but not always; the information may be known, but just not to the government, or it may be in plain view, but meaningless without a "search" for patterns and inferences to draw therefrom.[213] Two, that the text's "secure" is commensurate with "private." That is also often true in the physical world; Maureen Brady has shown that, historically, the desire for security against government intrusion that inspired the Fourth Amendment was commensurate with the desire for security against private parties' common law trespasses on private property that resulted in damage or unauthorized use.[214] It follows that efforts that we make to keep something "secure" against threats posed by our neighbors would apply via the Fourth Amendment equally to the government. In the physical world, that naturally often means keeping our papers and things *hidden* from neighbors, and thence

[212] *Supra*, text accompanying notes 192-99. My goal here is not to endorse any possible alternative value to privacy or claim that Fourth Amendment jurisprudence should find and effect the Amendment's "true" purposes. Instead, I want to show how blockchain expands on scholarly suggestions of alterative values.

[213] *See* Jim Harper, *Administering the Fourth Amendment in the Digital Age* 16 (National Constitution Center, A Twenty-First Century Framework for Digital Privacy, White Paper Series, 2017) ("In some cases, government agents may look so intently for something already exposed that the effort is a 'search.' . . . Search can also exist if government agents intensely examine exposed things."). *See also id.* at 24 ("[T]he use of outré technologies and techniques may signal a 'purpose of finding something' that is a search, even if the thing is unconcealed.").

[214] Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 951-52 & nn.13, 987-994 (2015). The point especially makes historical sense: regular police forces did not exist in the 18th century, and fellow-citizens were the main investigators and enforcers of public order. Stuntz, *Privacy's Problem*, *supra* note 168, at 407.

government. Blockchain's idiosyncratic architecture, however, forces us to face squarely how open, distributed data can be "secure" within the meaning of the Fourth Amendment, even if they are not "private" under the traditional *Katz* framework. To see how, consider how blockchain's structure confounds three black-letter rules from *Katz* and its progeny: the inside/outside and content/non-content distinctions, and the third-party doctrine.

A. *Inside/Outside*

Katz's emphasis on what is exposed to the public created a foundational distinction between objects and activities "inside" protected spaces, such as the house, and those "outside."[215] But what, precisely, is the reasoning behind that distinction? The answer, once we stop to think about it, is an unspoken intuition of living in a three-dimensional world, that we normally keep things secure from prying eyes by keeping them inside. Fourth Amendment rights as against law enforcement are actually defined by rights as against private strangers, what Jed Rubenfeld calls the "Stranger Principle": "[T]hat which we have exposed to perfect strangers, we cannot claim to be private . . . [and t]o the extent we have opened something otherwise private to a perfect stranger, the police may intrude into it as well."[216]

The Stranger Principle has been sharply critiqued on the grounds that most people reasonably do not invite the police to see everything that they choose to show their neighbors,[217] and that the principle loses force in the digital world in which "exposure" is so much more far-reaching than merely opening one's window in view of the neighborhood.[218] Blockchain complements both criticisms, of course, but also makes us think carefully about why people hide things at all. People value privacy for multiple reasons, and privacy can have substantive value apart from instrumental uses.[219] But often, people are not (strictly speaking) worried about a private thing's being seen by strangers. They are actually worried about what could happen *after* a private thing is seen. Untrustworthy people can

[215] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1009, 1011 (2009) [hereinafter Kerr, *Applying the Fourth Amendment*].

[216] Rubenfeld, *supra* note 154, at 110; *see also* Michael Mannheimer, *Decentralizing Fourth Amendment Search Doctrine*, 107 KY. L.J., 169, 174 (2019) [hereinafter Mannheimer, *Decentralizing*] ("[T]he line separating searches from non-searches is the behavior we expect from other private citizens regarding our security in our persons and property.").

[217] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting); Sherry F. Colb, *What Is a Search: Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002); State v. Earls, 70 A.3d 630, 643 (N.J. 2013) ("[N]o one buys a cell phone to share detailed information about their whereabouts with the police.").

[218] *See, e.g.*, Donohue, *supra* note 24, at 630-31; Rubenfeld, *supra* note 154, at 113-15.

[219] *See generally* Cohen, *supra* note 54.

then more easily damage or steal the thing, or embarrass us, or report our doings to others to our injury, and so on. Keeping a thing *private* from strangers in the physical world is the most practical *means* of effecting the *security* from strangers—and hence, through the Stranger Principle and Maureen Brady's insight, security from law enforcement—that we actually desire.[220] Privacy, that is, is oftentimes instrumental to security.[221]

In that light, *Katz*'s inside/outside distinction cannot quite grasp that security on blockchain is a function of openness and distribution, not privacy. Justice Harlan's claim that "objects, activities, or statements that [a person] exposes to the 'plain view' of outsiders are not 'protected'" would seem to deny Fourth Amendment coverage for public blockchain data. That is, until we consider his next words, "because no intention to keep them to himself has been exhibited,"[222] and we recognize that the reason blockchain users intentionally expose their data to specific anonymous others is to *maintain control of and protect* the data, the same intention that elsewhere motivates keeping things to one's self. Blockchain's unique architecture thus turns on its head Justice Harlan's assumption that what is inside and private is more secure from private invasion (and thus government invasion) than that which is exposed to others or seen. On a blockchain, the fact that strangers see data makes the data *more* secure from private harm, because their validation and inclusion on the immutable public chain means that untrustworthy people cannot thereafter damage or alter or steal them, while anonymity protects the user.

Moreover, blockchain throws off even the physical context from which *Katz*'s reasoning flowed. The opinion distinguished between what would have been Charlie Katz's *un*reasonable expectation of privacy from the uninvited eye (which could mark him through the phone booth glass) and his *reasonable* expectation of privacy from the uninvited ear, which he secured with the phone booth door.[223] The Court's language and reasoning about "privacy," that is, sprang from the physical facts of the case, and made perfect sense in the physical world in which the *security* of meetings, conversations, and telephone calls from phone booths correlated with their *privacy*. Things are quite different on a blockchain protocol. Instead, if we take the Stranger Principle seriously and treat exposure to strangers

[220] Ku, *supra* note 202, at 1370-71 ("What is important about the common law rule for natural senses is not its pedigree or its historical existence, but rather the reason for the exception. Natural senses are by default surveillance tools routinely used by the general public. The public, therefore, has always understood the threat to privacy and security represented by these senses and has responded accordingly by building walls and fences and prohibiting physical trespass. Technology should be no different.").

[221] *See* Clancy, *Property, Privacy, or Security*, *supra* note 152, at 344 (arguing that privacy analyses confuse "motivation for exercising the right to be secure with the right itself").

[222] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[223] *Id.* at 352.

as matching exposure to law enforcement, then in a blockchain environment the exposed data should become *more*, not less, protected from government invasion; they are put on a chain to become "secure" as against strangers. In effect, blockchain inverts the analytical work that *Katz's* conception of "privacy" and the inside/outside distinction normally would do in the physical world.

B. Content/Non-Content

A related black letter rule that blockchain inverts is the content/non-content distinction. The rule has its origins in the 1877 case *Ex parte Jackson*.[224] Jackson challenged the constitutionality of his conviction under a Congressional statute that banned any "letter or circular concerning lotteries" from being carried by mail.[225] The Court held that under the Fourth Amendment the government had no power to open "[l]etters and sealed packages" in the mail absent a warrant,[226] but that it could take evidence from parties who received the letters or were cognizant of what was in them.[227] "Exposed" materials could be prosecuted if contrary to morals (which did not, in the Court's mind, violate the First Amendment either): The "evidence respecting them is seen by everyone, and is in its nature conclusive."[228] The Court thus made a clear distinction (although without much explanation): that which was "sealed" was protected by the Fourth Amendment, while that which was "exposed" was protected, if at all, only by (a narrow) First Amendment.

This distinction is still generally in force,[229] slightly reframed via *Katz*. The "content" hidden within an envelope is protected until the recipient opens it and

[224] *Ex parte* Jackson, 96 U.S. 727 (1877).

[225] *Id.*

[226] *Id.* at 733. This statement may have been dicta: the Court did not apparently know whether the materials had been exposed or sealed; it ruled only on the question as the parties presented it, apparently presuming that the evidence had been obtained lawfully, and denied Jackson's request for relief. *Id.* at 736.

[227] *Id.* at 735.

[228] *Id.* at 736.

[229] The distinction is currently codified in the Wiretap Act, 18 U.S.C. §§ 2510-22 (governing contemporaneous interception of "content" not generally accessible to the public, for which a probable cause warrant is required) and the Pen/Trap Statute, 18 U.S.C. §§ 3121-27 (governing interception of "non-content," for which only a court order based on a showing of relevance to an investigation required). While this paper will not analyze privacy statutes closely, it seems unlikely that nonpermissioned nodes would qualify under the SCA as an "electronic communications service" provider or a "remote computing service" provider "to the public," which is an element of the Act's warrant requirement. *See* 18 U.S.C. §§ 2702(a)(1)-(3), 2703, 2510, 2711; United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) (a home computer connected to the internet is not an electronic communications service). It is a closer

destroys the sender's reasonable expectation of privacy through the Stranger Principle.[230] The outsides of envelopes—being exposed to the public—are not "content," and carry no reasonable expectation of privacy.[231] Courts have extended the analogy to withhold Fourth Amendment protection from other "non-content" such as pen registries of telephone numbers dialed[232] and the metadata (e.g., the "to" and "from") of emails,[233] while protecting the substance of the communications as "content."[234]

Scholars have hotly debated the merits of this distinction. Orin Kerr has argued that the content/non-content distinction is the proper digital analogue to the inside/outside distinction of the physical world.[235] But there is considerable room for doubt. The Amendment's text does not create the distinction; the *Jackson* Court seems to have intuited it reflexively from physical experience.[236] The distinction makes little sense in the digital world, in which data can easily change status between being metadata and content as the data move through complex layered network architectures.[237] Worse, in the digital world, superabundant

call whether either type of chain provides remote storage "to the public" as a service. *See, e.g.*, United States v. Standefer, No. 06-CR-2674-H, 2007 WL 2301760, at *14 (S.D. Cal. Aug. 8, 2007) (customers on an e-gold exchange did not use the website "to simply store electronic data" but "to transfer gold ownership to other users"); *but see* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1229-30 (2004) (concluding that eBay is not a remote computing service because "[t]he legislative history indicates that 'processing services' refer to outsourcing functions . . . This seems quite different from eBay: a user does not outsource tasks to eBay but rather uses eBay as a destination for the user's requests concerning buying and selling items"). These questions are outside the scope of this article, but at any rate, the Fourth Amendment may supersede the Act for shared non-content data that deeply implicate privacy concerns, as we will discuss momentarily. *Carpenter*, 138 S. Ct. at 2221. The SCA likely does not apply to traditional "content" data. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that defendant had reasonable expectation of privacy in the content of emails stored by third-party internet service provider and that the SCA was unconstitutional in permitting a warrantless search of them).

[230] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561, 582 (2009) [hereinafter Kerr, *Third-Party Doctrine*].

[231] *See, e.g.*, United States v. Van Leeuwen, 397 U.S. 249, 251 (1970).

[232] Smith v. Maryland, 442 U.S. 735, 745 (1979).

[233] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (holding that email to/from addresses and IP addresses are non-content).

[234] *Warshak*, 631 F.3d at 288.

[235] Kerr, *Applying the Fourth Amendment*, *supra* note 215, at 1020.

[236] Price, *supra* note 167, at 274 ("The text of the Fourth Amendment, however, does not actually draw a distinction between one's private papers and information about those papers, between data and metadata.").

[237] Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 57-59 (2016) (showing how, e.g., URLs or "From" email headers act as addressing information and as architectural content at different points in transit through network architectures).

metadata causes "non-content" quickly to morph into content as thousands of bits of metadata can collectively expose people's deepest secrets, by, for example, revealing patterns in their social contacts and affiliations.[238] Blockchain's lengthy and permanent ledger records—filled with metadata such as timestamps, patterns of use, transaction partners, and the like—naturally spark that same concern.[239]

But once again blockchain forces us to think even harder. Are public keys and digital signatures content or non-content? The key and signature are in one sense like a physical address, directing the transaction to a recipient.[240] But they simultaneously communicate the critical facts that the "user is who she claims to be and the message she is sending is authentic."[241] The "non-content" address data, moreover, grant a degree of privacy to the transaction as a whole, because the import of the transaction in most cases will be unintelligible unless connected to a person.[242] So too, as some have argued, cryptography *itself* acts as a closed container, shielding information from sight.[243] In the physical world, the outside of an envelope is visible to everyone, including law enforcement, while the inside content is hidden to keep it private and thus safe from prying eyes. But in blockchain's surprising architecture, the transactioners' addresses (traditional "non-content") are cryptographically sealed (and often tumbled to boot), while the transaction data (traditional "content") are visible—again, to make them immutable and secure.

All told, Blockchain in essence asks a court to analyze an analogy to a digital envelope whose traditional "insides" are visible and whose traditional "outsides" are locked and hidden. The content/non-content framework loses meaning on a blockchain once we realize that traditional content and non-content work together there to create security in personal information, without the secrecy that did the job in the physical world.

[238] *See, e.g.*, Alan Rusbridger, *The Snowden Leaks and the Public*, N.Y. REV. BOOKS (Nov. 21, 2013), https://perma.cc/76BA-3GZX; Donohue, *supra* note 24, at 556 ("Sophisticated pattern analytics mean that non-content morphs into content, making any formal distinction meaningless.").

[239] *See* Bacon et al., *supra* note 26.

[240] Pfefferkorn, *supra* note 188, at 1429-30.

[241] *Id.* at 1430-31 (citations omitted).

[242] *See* Lucas, *supra* note 14 ("Anyone can look at the Bitcoin ledger and see every transaction that happened, but the account information is a meaningless sequence of numbers.").

[243] *See, e.g.*, A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 871 (1995); Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L.J. 629, 672 (2000).

C. *Third Party, False Friend, and* Carpenter

The progeny of *Katz* for which blockchain data pose the biggest challenge are the third-party and false-friend doctrines, both of which are strong forms of the inside/outside distinction.[244] The third-party doctrine holds that a person has no reasonable expectation of privacy in information that he voluntarily exposes, not just to the public generally, but to *any* individual third party. "The concept of secrecy lies at the heart of the doctrine: what one keeps secret is private, while what one voluntarily exposes to others is no longer so."[245] The Supreme Court has explained that the doctrine rests on two rationales: a "reduced expectation of privacy in information knowingly shared" with others, and the "voluntary" nature of the exposure of information to others.[246] The false-friend doctrine goes a step farther: there is no reasonable expectation of privacy in information that one shares with another individual even with an express expectation that it will be kept in strictest confidence, on the rationale that one assumes the risk that one's compatriot might turn traitor and tell the police.[247]

At first glance, the two doctrines would seem a dart through the heart of Fourth Amendment protection for blockchain data. Every bit of data within a distributed ledger has necessarily been shared with some third party. On permissioned blockchains, data are usually shared among the enterprises that operate the blockchain together. On a nonpermissioned blockchain, users broadcast information to anonymous private owners of verifying nodes all around the globe to be published permanently for the entire chain to see. Even users who *subjectively* believe that their data have been shared securely because of blockchain's encryption and anonymity features might run afoul of the false-friend doctrine.

And yet, perhaps not. Given how blockchain upsets physical analogies, courts should not be knee-jerk in applying even familiar rules. The academy has

[244] Donohue, *supra* note 24, at 640-50.

[245] *Id.* at 640.

[246] *Carpenter*, 138 S. Ct. at 2210.

[247] Hoffa v. United States, 385 U.S. 293, 303 (1966); United States v. Miller, 425 U.S. 435, 443 (1976); Donohue, *supra* note 24, at 634 ("In undertaking criminal enterprises, one of the risks is that those with whom one deals are untrustworthy.").

almost[248] universally excoriated the doctrines,[249] particularly because in the modern world nearly every aspect of our lives from dawn to dusk intertwines with a device that delivers data about our doings to some third party, rendering the Fourth Amendment a solace solely for the Luddite.[250] Lower courts have pushed back as well.[251] And as of June 2018, after the landmark case *Carpenter v. United States*, the doctrines are apparently "on life support" at the Supreme Court.[252] Blockchain topples their rickety theoretical framework by showing that none of the rationales on which they rest survive the move to blockchain's digital space.

Carpenter was arrested in 2011 for robbing several electronics stores.[253] Part of the evidence against him was cell-phone tower locational data obtained pursuant to a warrantless court order to his wireless carrier; the data showed his cell phone had been near several of the robberies when they occurred.[254]

[248] I am not persuaded by Orin Kerr's arguments in rare defense of the third-party doctrine, Kerr, *Third-Party Doctrine*, *supra* note 230, particularly as would regard blockchain. Kerr first argues that the doctrine maintains "technological neutrality" because without it, technologically "savvy wrongdoers could use third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection," for instance by using electronic communications as substitutes for physical meetings of conspirators where the members might be seen. Kerr, *Third-Party Doctrine*, *supra* note 230, at 574-76. Node operators on blockchains are not co-conspirators being used as "cover," which at most derives from the private use of cryptography. Moreover, the doctrine is so devastating to the civil liberties of millions of citizens that it does not balance against the need to catch a few computer-savvy criminals. SOLOVE, *supra* note 167, at 109. Second, Kerr argues that the doctrine provides "ex ante clarity" because under the doctrine "Fourth Amendment rules are determined by information's knowable location rather than its unknowable history." Kerr, *Third-Party Doctrine*, *supra* note 230, at 565. Blockchain, however, poses the opposite situation—its "location" is nowhere and everywhere, while its history is already embedded in every block. Clarity, at any rate, is not virtue when it eviscerates a constitutional right. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2263-64 (Gorsuch, J., dissenting) (critiquing the clarity argument).

[249] *See, e.g.*, Kerr, *Third-Party Doctrine*, *supra* note 230, at 563 ("A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote."); Richards, *supra* note 151, at 1445 n.6 (collecting critiques of the third-party doctrine in the digital context); Strandburg, *supra* note 151, at 616 n.10 (collecting critiques).

[250] *See, e.g.*, *Jones*, 565 U.S. at 417-19 (arguing that the third-party doctrine "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") (Sotomayor, J., concurring); Donohue, *supra* note 24, at 640-41 ("In the contemporary world, it is impossible to live one's daily life without entrusting a significant amount of information to third parties. To say that we therefore voluntarily assume the risk that such information will be made public denies the role that technology plays.") (footnotes omitted).

[251] *See, e.g.*, *Warshak*, 631 F.3d 266.

[252] *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

[253] *Id.* at 2212.

[254] *Id.*; *Carpenter* thus represents a "carve-out" to the Act for certain kinds of data. Longman, *supra* note 95, at 111, 130.

Carpenter argued that the court order violated the Fourth Amendment.[255] The Court acknowledged that the cell-phone tower data were created by and shared with the third-party carrier, similar to the phone and bank records at issue in the seminal third-party doctrine cases *Smith v. Maryland* and *U.S. v. Miller*.[256] But it also acknowledged that "this sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents," and held for Carpenter, identifying and distinguishing the third-party doctrine's traditional twin rationales: the aforementioned "reduced expectation of privacy in information knowingly shared" with others, and "voluntary exposure."[257]

First, the Court emphasized that the doctrine depended not "solely on the act of sharing," but rather on the "nature of the particular documents sought."[258] Cell-phone data were "qualitatively different" from information shared in phone and bank records, because they conveyed "a detailed and comprehensive record" of a person's movements.[259] The Court emphasized that "the retrospective quality of the data here gives police access to a category of information otherwise unknowable."[260] Instead, the data were an "entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers."[261] Second, the majority denied that Carpenter "truly 'shared'" the data with his cell phone company voluntarily or "assumed the risk" of turning his data over; in the modern world, cell phones are "indispensable to participation in modern society" and automatically create a data trail in their wake.[262] The Court stressed, however, that its holding was narrow and did not upset the doctrines of *Smith* and *Miller*,[263] requiring a warrant only in "the rare case where the suspect has a legitimate privacy interest in records held by a third party."[264]

[255] *Carpenter*, 138 S. Ct. at 2206.

[256] *Id.* at 2216 (citing Miller v. United States, 425 U.S. 435, 440, 442-43 (1976)) (finding no legitimate expectation of privacy in bank records "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," even if "revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed"); *Smith*, 442 U.S. at 742-44 (1979) (finding no reasonable expectation of privacy in numbers dialed because "all telephone users" realize that the numbers they dial are shared with the phone company, and concluding that the "Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties").

[257] *Carpenter*, 138 S. Ct. at 2210, 2214.

[258] *Id.* at 2219.

[259] *Id.* at 2216-17.

[260] *Id.* at 2218.

[261] *Id.* at 2222.

[262] *Id.* at 2220.

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

[264] *Id.* at 2222.

The dissents of Justices Kennedy, Thomas, and Alito emphasized that Carpenter did not create, possess, or control the records (although they suggested that a person might retain an expectation of privacy in items merely bailed to a third party).[265] These dissents also noted a glaring inconsistency: the majority protected cell phone "locational" data, while still applying the third-party doctrine to financial data such as credit card statements and bank accounts, whose "vast scope" can reveal the privacies of life just as easily.[266]

Justice Gorsuch's dissent suggested an even more dramatic prescription. Noting that the Court had "never offered a persuasive justification" for the third-party doctrine, he also denied that tort law's "assumption of risk" had any bearing on criminal law, or that people consent to the government looking at papers when they give them to their friends.[267] He instead suggested entirely abandoning the "unpredictable—and sometimes unbelievable—jurisprudence" that *Katz*, *Smith*, and *Miller* spawned, and substituting another framework in which data owned under common law or positive law principles would retain Fourth Amendment protections even if shared.[268]

All told, "narrow" though it was, *Carpenter* suggested four things relevant here. First, that comprehensive data of a person's activities that evoke a fear of "near perfect surveillance"[269] or "arbitrary government power" will likely enjoy Fourth Amendment protection, even if created or held by third parties. (If perfect surveillance is the fear, moreover, then perhaps a future case will squarely rethink comprehensive surveillance of financial data.)[270] Second, data "shared" only because of the necessities of modern digital life will also forestall the third-party doctrine. Third, at least six current Justices are prepared to abandon the interpolation of tort law's "assumption of risk" into Fourth Amendment law. Fourth, four Justices all but begged Carpenter to show that he had some ownership interest in the data and, at least for Justice Gorsuch, that fact would trigger Fourth Amendment protection, whether the data were also held by third parties or not.[271]

[265] *Id.* at 2223, 2227, 2228, 2230, 2257 (dissents of Kennedy, Alito, and Thomas, JJ.).

[266] *Id.* at 2232-33.

[267] *Id.* at 2263 (Gorsuch, J., dissenting).

[268] *Id.* at 2266, 2269-71 (warning, however, against swinging too far back to the broad sweep of *Boyd*).

[269] *Carpenter*, 138 S. Ct. at 2210.

[270] *See* Andrew G. Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (Jun. 25, 2018), https://perma.cc/A57R-XBEV [hereinafter Ferguson, *Future-Proofing*].

[271] Orin Kerr has provided a similar roadmap for considering *Carpenter*. He would ask three questions: does the technology at issue record data in a way not possible before the digital age in terms of bulk, easy recall, and analysis? Does a person share the data without any meaningful voluntary choice? Do the data reveal the privacies of life? If the three boxes are checked, Kerr would call an examination of the data a *Carpenter*-source search requiring a warrant. Orin S. Kerr, *Implementing* Carpenter (USC Law Legal Studies Paper No. 18-29, 2019).

Now consider how such a Court might scrutinize blockchain data. The analysis would be specific to the architecture in question.[272] Permissioned, enterprise blockchains that sweep up thousands of people's daily activities comprehensively (perhaps through the Internet of Things or autonomous vehicles or some pervasive blockchain-based application) would be a close analogy to *Carpenter*, particularly if the data are "shared" from quotidian devices. That analogy will only grow stronger as blockchains become omnipresent, recording intimacies such as where we drive and what we order from our smart speakers.[273] Indeed, the *Carpenter* Court was careful to note that it "must take account of more sophisticated systems that are already in use or in development."[274]

Open blockchains would be a harder question at first glance. The choice to use them is (at least right now) far more voluntary than owning a cell phone, and cryptocurrency protocols particularly are not comprehensive windows into a person's life and movements; instead, they are now much more like bank records. Yet that may change if cryptocurrency use becomes widespread, or if a majority of the Court takes a hint from the dissents and finds an on-point case to patch over the inconsistency of protecting comprehensive physical movements but not (possibly even more) sensitive and comprehensive financial information.

More important, while *Carpenter* still spoke the language of "privacy," it really recognized in its rejection of the third-party doctrine's traditional rationales a deeper Fourth Amendment premise: security against arbitrary government invasion into one's massed digital data. Blockchain helps realize that premise: it is also an "entirely different species of business record" that, by its nature, "implicates basic Fourth Amendment concerns about arbitrary government power."[275] Blockchain ledgers were consciously designed to create security, especially against government control.[276] Blockchain also impeccably embodies the kind of "historical" records that several Justices feared give "police access to a category of information otherwise unknowable;"[277] a search of an immutable blockchain could instantly reveal years of activities, edging us closer to "near perfect surveillance," especially, again, as blockchain uses become ever more pervasive and scrupulously and permanently record when, where, and what we

[272] *See* Bacon et al., *supra* note 26, at 213 ("Given the diversity of possible blockchain platform designs, . . . each application of blockchain technology will need to be considered on its facts.").

[273] *See* Longman, *supra* note 95, at 130.

[274] *Carpenter*, 138 S. Ct. at 2213 (quoting *Kyllo*, 533 U.S. at 36).

[275] *Id.* at 2222.

[276] *See* Longman, *supra* note 95, at 131 ("[T]he platform itself was created to provide more secure and anonymous transacting, proliferating among users in the deep and dark webs, and allowing for a system of anonymity.").

[277] *Carpenter*, 138 S. Ct. at 2218.

are doing.[278] As a purely technical matter, blockchain ledgers also act like cell phone data in that "hash connections are similar to the constant connections phones make to cell sites. Cell phones constantly search for signals, even when the phone is not in use by its owner. Likewise, blockchain ledgers connect transactions to other transactions both before and long after the user makes his own transaction."[279] Further, a majority of Justices seem poised to excise from Fourth Amendment law the ill-fitting "assumption of risk" import from tort; blockchain has undone even *tort's* anterior rationale, structuring its transactions so that its users *do not have to* assume any risk of placing trust in others.[280] Finally, several members of the Court would seem receptive to the argument that people's blockchain data, though shared with and held by other nodes, are still in a sense *theirs*—created by them and, especially in the case of cryptocurrencies, *controlled* exclusively by their private keys, an issue we will explore further below.[281] In all, blockchain's unique architecture undercuts the traditional rationales of these shaky doctrines, and shares the reasoning of *Carpenter*'s attack on them.[282]

What follows? Should the demise of these distinctions and doctrines mean that the government be restricted from looking at a blockchain's shared, open data? That would require a leap from current doctrine and prompt several sensible objections. One is that it is deeply unreasonable to ask the government

[278] *Id.* at 2210.

[279] Longman, *supra* note 95, at 133.

[280] Antonopoulos, *supra* note 122 (noting that a distributed "network no longer needs to be closed, access-controlled or encrypted. Trust does not depend on excluding bad actors, as they cannot 'fake' trust. They cannot pretend to be the trusted party, as there is none. They cannot steal the central keys as there are none. They cannot pull the levers of control at the core of the system, as there is no core and no levers of control.").

[281] *Infra* Part III.E.

[282] A few final thoughts on blockchain and the third-party doctrine. First, the *Carpenter* Court was badly fractured, with four separate dissents. A litigant would have to corral numerous arguments to marshal a majority about a different technology—but blockchain touches enough key issues to cobble one together. Second, the third-party doctrine has been defended on the grounds that it treats the third party as a free actor, able to share what they wish. Stephen E. Henderson, Carpenter v. United States *and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL RTS. J. 495, 524-25 (2017). That may be true, but on blockchains this issue is muted: the parties are usually anonymous, and an informer's information would likely be limited to what the chain could already see anyway. Third, scholars have worried that without the clarity of the doctrine, we are left with judging infinite gradations of secrecy. *See, e.g.*, Kerr, *Third-Party Doctrine*, *supra* note 230, at 1080. That concern also is muted on a blockchain, in which privacy and anonymity are clearly switched on for addresses and keys, and off for data. Fourth, if the *Carpenter* dissents are correct that the Fourth Amendment should rest on positive law such as property, blockchain would have to admit some place for Leviathan, which may be difficult for some of its enthusiasts to swallow. But the idea that blockchain is never to interact with regular law is seriously misguided anyway. WERBACH, BLOCKCHAIN, *supra* note 2, at 158 ("The experience of the past twenty years suggests that governments and very powerful private institutions will not so easily be disintermediated.").

not to look at a publicly available document. As Laura Donohue puts it, "if any citizen could witness others' behavior, why should government officials, who also happened to be present, not be allowed to do the same?"[283] There are a few responses. Donahue's answer to her question in a three-dimensional world is the "absurdity of directing people to close their eyes, avert their gazes, or otherwise ignore their senses."[284] But although it is absurd to expect people in the physical world to avert their gaze from an exposed public object or activity, blockchain data are not a fair analogy to just some act on the street. One has to go looking for blockchains, and must (at least as present) have quite a bit of sophistication to analyze and make sense of the data.[285] Again, the necessary complex analytics (currently the realm only of experts) act like a form of specialized sensory enhancement, which should trigger Fourth Amendment protections.[286] It may be, to be sure, that a single, brief look at blockchain data will differ in "reasonableness" from lengthy surveillance.[287] But it also seems likely that law enforcement will rarely be satisfied with a brief, targeted look alone.[288] Rather, because of the growing pervasiveness of data, of which blockchain is a driver, some scholars have directly suggested that government does need to learn to avert its digital "eyes" from all that can be seen, lest the Fourth Amendment become vestigial.[289]

Another objection might be that blockchain's architecture *expects* that the government will look (or at least does not demand that it should not), and so the Fourth Amendment should not be triggered if the government in fact *does* look. That objection, however, subconsciously slips back into the much-maligned circularity of the *Katz* test, imagining that expectations should dictate Fourth Amendment coverage, which then molds expectations. Expectations, rather, might be wholly irrelevant to whether the Fourth Amendment should or does

[283] Donohue, *supra* note 24, at 560-61.

[284] *Id.* at 561.

[285] *See* Andrew G. Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 583 (2017) [hereinafter Ferguson, *Smart Fourth Amendment*] (arguing that information from smart devices is not "really in 'plain view.' Special devices are needed to intercept it, and data are rarely immediately incriminating, since the transmissions reveal nothing without translation and analysis").

[286] *Supra*, note 129.

[287] *See* Slobogin, *A Defense of Privacy*, *supra* note 158, at 160 ("[C]ourts should recognize a [privacy-related] right to anonymity or obscurity in public, but that the strength of this interest depends on the length of the public monitoring, the degree to which the police take steps to record public activities, and so on.").

[288] David C. Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 63, 92 (2013) (noting that law enforcement has a natural, "teleological tendency toward a surveillance state," against which the Fourth Amendment is a "bulwark").

[289] Ohm, *supra* note 172, at 1353-55.

protect information.[290] And to paraphrase Justice Gorsuch's argument above, simply because users invite other nodes to view their transactions to effect the ends of security does not mean that they invite the government to look, even if they contemplate or expect that it might.[291]

A final objection might be that while people may reasonably expect their blockchain data to be "secure" against tampering, that kind of "security" is not what the government is invading. The government is not trying to tamper with the data or destroy it, but simply to look at it, which blockchain does not prohibit. But this reasoning only underscores that "privacy" is often a means to other ends—security or control of one's things in particular. Under current doctrine, the government is bound to respect privacy as the necessary means to effect many purposes, including security and control. On a blockchain, visibility and distribution are the necessary means to those same ends of security and control of data, which are also met in the totality of the transaction—part public so that the other nodes can process it, part private so that the person is not identified. Why should the government be permitted to exploit with impunity the new means to constitutionally protected ends, simply because the physical-world middleman has changed?[292] And can the Fourth Amendment really not see the difference between sharing data in an effort to improve upon attaining longstanding human desires, and giving government a license to scan what people are doing, indiscriminately, at leisure, forever?[293]

I suggest that the Amendment can easily see the difference; the difference remains obscure only if we remain in *Katz*'s ruts and insist that privacy is a talisman, an on-off secrecy switch. Blockchain invites us to think counterintuitively. If one of the Fourth Amendment's purposes is to vindicate "security" against government intrusion, and if that "security" shares, as it does,

[290] *See* Tomkovicz, *supra* note 160, at 679-80 (noting that other fundamental rights do not normally hinge on "the expectations of potential claimants").

[291] *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).

[292] *See* Gray & Citron, *supra* note 288, at 140-41 ("Much of the hope and promise of networked technologies is that they expand the horizons of our personal explorations and associations while providing diverse forums for civil society engagements that would otherwise be impractical or impossible. That potential would be severely compromised if we knew the government was or well might be watching everything we read, write, or do in the digital world.").

[293] Paraphrasing Sundby, *supra* note 152, at 1793; *see also* Steven T. Snyder, *The Privacy Questions Raised by Blockchain*, LAW 360 (Jan. 14, 2019), https://perma.cc/C5RE-YSFC ("Once attributed to an individual through any means, a lifetime of pseudonymous transactions will be permanently exposed as linked to that person."); Gray & Citron, *supra* note 288, at 102 (arguing that the fact that a particular search is limited should not matter if the "challenged technology is capable of broad and indiscriminate surveillance by its nature, or is sufficiently inexpensive and scalable so as to present no practical barrier against its broad and indiscriminate use," at which point "granting law enforcement unfettered access to that technology would violate reasonable expectations of quantitative privacy").

the same sense in which we historically achieved "security" from our neighbors, then blockchain shows us that Fourth Amendment security can be had without privacy-as-secrecy. Doctrine should develop to reflect that reality.

2. *Expression and Association*

Security, at any rate, isn't the only value in play. Any attempt to grapple with the Fourth Amendment's meaning must take into account its original close relationship with the First Amendment.[294] Two prominent cases from England during the colonial period—*Wilkes v. Wood*[295] and *Entick v. Carrington*[296]—are generally recognized as precursors to the right against unreasonable searches and seizures.[297] Both cases involved a similar fact pattern: royal officials ransacked the houses of suspected libelers in an attempt to squelch scurrilous written attacks on King George III's government—in Entick's case with a particularized warrant, but in Wilkes' case with a general warrant to search any place where evidence might be found that failed specify whose houses might be invaded, what evidence might be seized, or who might be arrested.[298] The perturbed arrestees sued the King's officials for trespass, on the theory that the warrants—which otherwise immunized the officials from suit—were illegal, and they won massive verdicts from indignant juries.[299] These cases have long influenced Supreme Court Fourth Amendment analyses.[300]

Of course, the cases were "classic First Amendment cases in a system with no First Amendment, no vehicle for direct substantive judicial review."[301] They were as much a part of the First Amendment story as about general warrants and intrusive government searches. The Fourth Amendment's obstacles to searches and seizures, in other words, protected papers and houses in order to protect the ideas and gatherings they contained:

[294] *See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007) [hereinafter Solove, *First Amendment*].

[295] (1763) 98 Eng. Rep. 489 (C.P.).

[296] (1765) 95 Eng. Rep. 807 (C.P.).

[297] Price, *supra* note 167, at 252-55; Ku, *supra* note 202, at 1333-35.

[298] While Entick's particularized warrant would be permissible under the modern Fourth Amendment, it was impermissible in the "more libertarian," "anti-government" framework of the era. George Thomas, *The Common Law Endures in the Fourth Amendment*, 27 WM. & MARY BILL RIGHTS J. 85, 95 (2018).

[299] *Id.* at 94.

[300] *See, e.g.*, Boyd v. United States, 116 U.S. 616, 626 (1886); Clancy, *Property, Privacy, or Security*, *supra* note 152, at 310-26 (showing Entick's influence on Fourth Amendment doctrine).

[301] Stuntz, *Privacy's Problem*, *supra* note 168, at 403.

> By design, therefore, a paramount purpose of the Fourth Amendment was to serve as a guardian of individual liberty and free expression. In other words, it was intended to function as a barrier to government overreach and as a catalyst for other constitutional rights, notably freedom of speech and freedom of association, which are essential to a healthy democracy.[302]

The original connection between the Amendments survives in case law today: the Supreme Court recognizes that the Fourth Amendment must be applied with "scrupulous exactitude" when significant First Amendment rights are implicated by a search.[303] It follows, scholars have argued, that in the digital realm the Fourth Amendment protects more than privacy; it protects a right to digital expression and association in all manner of digital communications among persons.[304]

There is of course an essential tension between the Fourth Amendment's current focus on "privacy-as-secrecy" and the First Amendment's freedom of speech and association. "Expressive freedom, associational rights, and interests in 'personal autonomy' can often be fully taken advantage of *only* by engaging in somewhat revelatory behavior—that is, conduct that makes information about one's affairs more accessible to others, including the government."[305] But knowledge that shared information can be searched at will can lead to self-censorship.[306] In the physical world, the best defense to censorship is to publish to intended readers but to hide from the government—a tall order.

[302] Price, *supra* note 167, at 257-58; *see also* Richards, *supra* note 151, at 1450-51 (noting the "linkage between the Fourth and First Amendments," and concluding that "[t]he recognition of express protection for 'papers' should thus best be understood as an attempt to place a substantive limit on government power primarily in the context of communications and dissent.") .

[303] Stanford v. Texas, 379 U.S. 476, 485 (1965); *see also* Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978); New York v. P. J. Video, Inc., 475 U.S. 868, 873 (1986). The Privacy Protection Act, 42 U.S.C. § 2200aa prohibits searches of "work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication," except under specific circumstances, in which case a warrant is required.

[304] *See, e.g.*, Price, *supra* note 167, at 283-86 ("[T]he content of communications, whether spoken, typed, or beamed over the Internet, are the kind of expressive and associational materials that the Framers intended to shield from arbitrary search and seizure through the Fourth Amendment."); Richards, *supra* note 151, at 1487-88 ("In translating the Fourth Amendment to the cloud, . . . Fourth Amendment protection should be strongest when dealing with social and technological activities that are intertwined with a First Amendment value.").

[305] Tomkovicz, *supra* note 160, at 682-83 (emphasis in original).

[306] *See, e.g.*, Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117 (2016) (empirical study providing "evidence of regulatory 'chilling

Blockchain helps resolve this dilemma; its immutable ledger and cryptographic anonymity can help keep speech robust by being sharable and censorship-resistant at once. Censorship resistance and free information flow were a large part of blockchain's *raison d'être*.[307] Blockchain companies specifically tout these traits. The internet company Alexandria, for example, is working on a massive open-index protocol—a way to structure the internet so that private platforms do not monopolize information into silos but share it in a giant database—using blockchain architecture; this would permit decentralized, open indexing of enormous amounts of data without censorship, creating "a public space on the internet for all information."[308] A quick look around the world shows the potential value of such a project, as Chinese citizens are using Ethereum-based blockchains to circumvent government expurgation of the news.[309] Blockchains provide protections not just from government censorship outright, but from hackers and single points of failure for information flows.[310] Commentators even suggest that cryptocurrencies provide a defense against government financial blacklists that might squeeze dissidents.[311]

Of course, just because blockchain resists censorship does not mean that its users are perfectly immune from being found and punished. Blockchain lessens but does not eliminate the chilling potential, which means that the Fourth Amendment still has work to do. That concern may seem a bit moot in a nation of currently robust free speech. All the same, Wilkes or Entick would probably have jumped at the chance to publish anonymously on a censorship-proof platform, and there remain serious authoritarian implications if governments can simply peruse years' worth of data on immutable open ledgers at their pleasure.[312]

effects' of Wikipedia users associated with online government surveillance"); Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH L. REV. 465, 518 (2015) (noting empirical studies suggesting that "anxiety about government monitoring could influence participation in politics, political criticism, and voter decision-making"). *But see* Sklansky, *Too Much Information*, *supra* note 177, at 1094-1101 (questioning empirical evidence of self-censorship).

[307] WERBACH, BLOCKCHAIN, *supra* note 2, at 158.

[308] *See* ALEXANDRIA, https://perma.cc/2Q7D-HD4K (archived Dec. 26, 2019) (and embedded video).

[309] Nir Kshetri, *Chinese Internet Users Turn To the Blockchain To Fight Against Government Censorship*, THE CONVERSATION (Feb. 25, 2019), https://perma.cc/BFB5-U6ST. To be sure, the Chinese government is fighting back, attempting to regulate all blockchain use in China. Yogita Khatri, *China's Internet Censor To Start Regulating Blockchain Firms Next Month*, COINDESK (Jan. 10, 2019), https://perma.cc/3V24-38SB. The denouement remains to be seen.

[310] *Supra*, text accompanying notes 151-52.

[311] Mick Hagen, *Blockchain Could Be the Savior of Free Speech*, FORTUNE (Jul. 26, 2018), https://perma.cc/GJV3-YYUL.

[312] *See* WERBACH, BLOCKCHAIN, *supra* note 2, at 159 ("The universal visibility of transactions in a distributed ledger is an authoritarian regime's dream.").

If the Fourth Amendment is not capacious enough to address these concerns, it has lost its original moorings. In effect, blockchain challenges the Fourth Amendment to live up to its First Amendment kinship. A court considering a search of data on a blockchain, especially one used for information-sharing, and particularly in an attempt to find the publisher, should not, again, react in a knee-jerk manner just because the data may not be kept totally secret.[313] Rather, the blockchain may be substantializing deeper values of expression and association within the Fourth Amendment's DNA that privacy-as-secrecy has long forgotten. Courts must use caution.

3. Economy and Autonomy

Although First Amendment implications might be quite relevant for information-sharing platforms, they may not apply to more purely commercial platforms such as cryptocurrency protocols.[314] But there is one further historical and theoretical Fourth Amendment value at play here. In addition to the *Entick* and *Wilkes* libel cases, the Fourth Amendment was born of the colonists' experience with "intrusions on commercial conduct: searches aimed at uncovering goods smuggled into the colonies without paying appropriate excise taxes."[315]

"It is not too much to say that Boston's economy in [the colonial] period was grounded on an illegal trade," particularly in molasses for making rum.[316] The exasperated royal reaction was the infamous "writ of assistance," which permitted broad searches of any premises for smuggled goods.[317] The writs "were called writs of assistance because they commanded all officers and subjects of the Crown to 'assist' in their executions. The writ, therefore, was not, strictly speaking, a search warrant, but it functioned as one."[318] The colonists were furious. In 1763 James Otis famously inveighed (in vain) against the writs in Boston Superior Court on behalf of some merchants (or, rather, smugglers),[319] and John Adams—

[313] *See* Solove, *First Amendment*, *supra* note 294, at 160 (suggesting a tailoring scheme in cases involving government searches of materials with First Amendment implications).

[314] *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 567 (2011) ("[R]estrictions on protected expression are distinct from restrictions on economic activity or, more generally, on nonexpressive conduct.").

[315] Lvovsky, *supra* note 160, at 1213.

[316] Stuntz, *Privacy's Problem*, *supra* note 168, at 404-05.

[317] Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHICAGO L. REV. 1181, 1242 (2016).

[318] Wasserstrom & Seidman, *supra* note 157, at 81 n.251.

[319] *Id.* at 55.

who was present—identified Otis' attacks with the spirit of revolution: with Otis' speeches, Adams wrote, "the child Independence was born."[320]

When that "child" reached maturity, the Founders remembered the context of its birth.[321] Adams' experience with the writs undergirt his draft of the Massachusetts Declaration of Rights' protections against searches and seizures, which served as a precursor to the Fourth Amendment.[322] The Constitutional ratification debates repeatedly hearkened back to the writs of assistance; prominent anti-federalists proposed to reject the proposed compact because unconstrained federal excise officers would ransack citizens' homes for commercial contraband.[323] Early Fourth Amendment cases, particularly *Boyd*, showed a special solicitude for economic interests, rather than for "privacy" as intimacy or secrecy.[324] As Anna Lvovsky has argued,

> Historically . . . the Fourth Amendment's protections against unreasonable seizure were not seen as protecting anything so narrow as intimacy or domesticity. They were envisioned as a broad bulwark of individual sovereignty, safeguarding an individual's personal property, commercial freedoms, and political beliefs. At the time of the Amendment's enactment, its primary concerns included commercial sites like warehouses and business fronts—as well as, quite centrally, papers, including business records, as uniquely precious windows into a man's secret thoughts. [325]

Three lessons follow. First, as a secured business record, blockchain resonates with the Fourth Amendment's historical close relationship with economic activity.[326] Second, it shouldn't put us off that people can and do use blockchains for illegal purposes; anger at unfettered royal searches for (rampant)

[320] Thomas Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 1005 (2011) [hereinafter Clancy, *The Framers' Intent*].

[321] *Id.* at 88.

[322] Clancy, *Property, Privacy, or Security*, *supra* note 152, at 1052.

[323] *See, e.g.*, Luther Martin, *Genuine Information VI*, BALT. MD. GAZETTE (Jan. 15, 1788), *reprinted in* 15 THE DOCUMENTARY HISTORY OF THE RATIFICATION OF THE CONSTITUTION 377 (John P. Kaminski & Gaspare J. Saladino eds., 1984) (evincing fear of federal exise officers); George Mason, *Debates, The Virginia Convention* (June 11, 1788), *reprinted in* 9 THE DOCUMENTARY HISTORY OF THE RATIFICATION OF THE CONSTITUTION, *supra*, at 1157 (same).

[324] Cloud, *Privacy, Property, and Liberty*, *supra* note 140, at 576 (noting that *Boyd* "defined a man's sacred 'privacies,' quite loosely, as his 'indefeasible right of personal security, personal liberty, and private property.'") (internal citations omitted).

[325] Lvovsky, *supra* note 160, at 1239.

[326] *Id.* at 1216 ("[T]he Supreme Court's initial Fourth Amendment cases emphasized an individual's interest in his commercial pursuits and personal papers more than his intimate or familial bonds.").

rum-running begat protections that now redound to the general public.[327] Third, the economic freedom that blockchain claims to offer is part of yet another Fourth Amendment value, personal autonomy.

Autonomy is a bit hard to define; it is variously described as a right to engage in a chosen commercial or economic activity,[328] as well as self-development, the ability to engage in "unorthodoxy, self-definition, and retreat"[329] from the pressures of communal society, the right to "attend to one's desires and personal fulfillment,"[330] and a "principle of self-sovereignty."[331]

Perhaps the most elevated expression of the idea comes from Justice Brandeis' dissent in *Olmstead*. Brandeis complained that majority's narrow, physical-trespass-based rule failed to contemplate how the Fourth Amendment's defense of self-direction could be applied to modern technology:

> The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions . . . Can it be that the Constitution affords no protection against such invasions of individual security?[332]

To Brandeis, the Fourth Amendment defended "man's spiritual nature . . . his feelings and of his intellect."[333] The Founders "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[334] Notably, privacy was *instrumental* to this "right to be let alone": "*To protect that right*," Brandeis wrote, "every unjustifiable intrusion by the government upon the privacy of the

[327] *See* David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. 425, 462 (2016) (noting that although few colonists were subjected to the writs, they "posed a general threat to the freedom and security of all in their persons and property").

[328] Lvovsky, *supra* note 160, at 1212.

[329] *Id.* at 1262.

[330] *Id.* at 1240.

[331] *Id.*

[332] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

[333] *Id.* at 478.

[334] *Id.*; *see also* Lvovsky, *supra* note 160, at 1239 ("Early understandings of the Fourth Amendment did not aim to protect a right of domesticity or intimate retreat from the state, and certainly not to encourage orthodox behaviors. They protected the individual's right to disagree with political and social orthodoxy.").

individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[335] In other words, to Brandeis, the Fourth Amendment advanced a packet of constitutional goals, such as autonomy, self-expression, control of property and commercial activities, and repose, using privacy as a trigger mechanism.[336] (It should not be forgotten, either, that Brandies wrote these words in defense of a notorious bootlegger.)

Now, in the physical world, the right of autonomy or to be let alone means, at least in part, to have a way in which to situate yourself and your things so you won't be bothered. As should be obvious by now, blockchain also enables the same goal, but without so strict a need for perfect privacy-as-secrecy or physical boundaries, and also presents the very present possibility that governments can reach into our information or thoughts or beliefs without ever reaching into our houses or "secret drawers." That is, if the point of the Fourth Amendment is to give us breathing room and control to live our lives as we choose, with minimal external restraints, blockchain shares that vision and creates a digital system that aids it, but also creates the danger of government invasion that Brandeis predicted.

E. Text and History

All this talk so far of privacy and finding the Fourth Amendment's "true" values has probably had textualists grimacing. After all, if the Fourteenth Amendment does not "enact Mr. Herbert Spencer's Social Statics,"[337] the Fourth Amendment hardly enacts Satoshi Nakamoto's crytpolibertarianism—although the previous discussion shows that the Fourth Amendment historically and currently shares much with blockchain's animating theories. So let's finish with the third criticism of *Katz*: that it simply ignored the plain language of the Amendment. Even here, blockchain shows how computer data can act as a kind of property to be defended from unreasonable government incursion, without putting a thumb on the scale for the policy preferences of technolibertarians.

1. Papers and Property

Textualists advocate a step-by-step approach to the Fourth Amendment: identify a "person, house, paper or effect" belonging to the defendant, ask whether

[335] *Olmstead*, 277 U.S. at 478 (emphasis added).

[336] *See* Tomkovicz, *supra* note 160, at 667 ("[T]he main reason for constitutionalizing informational privacy is its instrumental role as a medium within which other rights and interests can survive, even flourish."); Slobogin, *A Defense of Privacy*, *supra* note 158 (arguing that privacy capably advances other suggested constitutional goals of the Fourth Amendment).

[337] Lochner v. New York, 198 U.S. 45, 75 (1905) (Holmes, J., dissenting).

a "search" within the ordinary meaning of the word occurred of that thing, then ask whether that search was "reasonable."[338] Blockchain records are almost certainly modern-day "papers," for which Fourth Amendment protections would apply; no one in *Carpenter*, at any rate, seemed to question the analogy for cell phone tower records.[339] Nor should it necessarily bother a textualist that a "search" can be for something technically seen or seeable but still opaque or mysterious, for which careful analysis and inference are required in the pursuit of evidence of crime.[340] Accessing blockchain data through a website like www.blockchain.com for a look around a ledger might, for example, be enough to constitute a "search" for some unknown (albeit easily accessible) information; all the more so if the access is to conduct lengthy analyses (which probably would be the most meaningful examinations in a criminal investigation anyway).[341]

"Reasonableness" is trickier. Under *Katz*, "unreasonable" means a warrantless search into a constitutionally protected space, absent some exigency.[342] But what does the *text* mean by "unreasonable"? There is some debate. Laura Donohue has offered substantial evidence that, for the Framers, "unreasonable search and seizure" meant a trespass contrary to common law,[343] while Thomas Davies has argued, slightly more narrowly, that "the Framers would have understood 'unreasonable searches and seizures'" as a "pejorative label for searches or arrests made under that most illegal pretense of authority—general warrants."[344] Other scholars argue that "unreasonable" meant just that, and was a balancing mechanism implanted into the Amendment,[345] or that the founders might have

[338] *See, e.g.*, Harper, *supra* note 213, at 31-32.

[339] *Carpenter*, 138 S. Ct. at 2230, 2269 (Kennedy, J., dissenting; Gorsuch, J., dissenting).

[340] *See Kyllo*, 533 U.S. at 33, n.1 (2001) (noting that a "search" could occur even in the "absence of trespass," quoting WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (1828) (reprint 6th ed.1989), defining search as "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection.") (original emphasis omitted, emphasis added); Epstein, *supra* note 136, at 38-39 ("The only requirement for a search is an effort—by either the unaided senses or any instrument or device, whether commonplace or exotic—to learn something that one did not know."); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551 (2005) [hereinafter Kerr, *Searches and Seizures*] (a digital search "occurs when information from or about the data is exposed to possible human observation") (emphasis added).

[341] *See* LR & Orr, *supra* note 104, at 6.

[342] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[343] Donohue, *supra* note 24, at 561, 682-83.

[344] Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 693 (1999).

[345] *See, e.g.*, David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1780 (2000) (doubting that the Fourth Amendment constitutionalized common law rules through the word "unreasonable"); Michael Mannheimer, *The Contingent Fourth Amendment*, 64 EMORY L.J. 1229, 1238 (2014); William Cuddihy, *Warrantless House-to-House*

felt that the word "unreasonable" enacted some common-law protections beyond merely banning general warrants.[346] But at all events, "[w]hether or not . . . the Framers intended only to ban general searches, it is clear that general searches were their principal concern."[347]

I cannot hope to resolve this debate here. I simply point out that if Donohue and Davies are convincing that the "unreasonable search" of the text originally meant approximately "a search in the nature of a general warrant, contrary to common law," then searches of blockchain data are quite problematic. A search of an open ledger could reveal information about the activities of thousands of people, indiscriminately, locked into the ledger over a course of years.[348] Data in one block are entangled with information about and in many others. There would also be no easy way to bound the search by a location; data from nodes worldwide would be effortlessly accessible in one spot. Think of Toyota's vehicle data.

A search of a blockchain, unless tightly restricted by a technically sophisticated judge and executed by sophisticated law enforcement officers, could turn very quickly into the functional equivalent of a quintessentially "unreasonable" general warrant to search thousands of people's information in thousands of places—an astounding opportunity for pretextual searches or "fishing expeditions," rendered all the easier by an argument that the data were sitting there to be seen.[349] As Orin Kerr has argued, the *ease* of search should change the calculus of whether to *permit* a search,[350] and radical changes to search ability should force changes to doctrine—including even eliminating the plain-

Searches and Fourth Amendment Originalism: A Reply to Professor Davies, 44 TEX. TECH. L. REV. 21. *But see* Davies, *Can You Handle the Truth?*, *supra* note 147, at 107 ("[T]here was no standard as flimsy as reasonableness in framing-era search doctrine, and the Framers did not intend to create any such broad standard. Indeed, they did not intend to do anything more in the Fourth Amendment than ban the issuance of general warrants.").

[346] *See* Clancy, *The Framers' Intent*, *supra* note 320, at 1061.

[347] George C. Thomas, *Stumbling Toward History: The Framers' Search and Seizure World*, 43 TEXAS TECH. L. REV. 199, 206 (2010); *see also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, MINN. L. REV. 131, 366 ("[T]he primary abuse thought to characterize the general warrants and the writs of assistance was their indiscriminate quality, the license that they gave to search Everyman without particularized cause").

[348] *See* ROCIC, BITCOIN AND CRYPTOCURRENCIES, *supra* note 13, at 15 ("The blockchain is of particular interest to law enforcement due to its inability to be altered in any way.").

[349] *See* Laura K. Donohue, *The Dawn of Social Intelligence (SOCINT)*, 63 DRAKE L. REV. 1061, 1102-11 (2015); Orin S. Kerr, *Opinion, Government 'Hacking' and the Playpen Search Warrant*, WASH. POST, https://perma.cc/9HJ5-7KGP ("Can a single warrant justify a search of thousands or even [hypothetically] millions of computers, all used by different people who don't know each other? At what point does the use of a single warrant to search many places make the warrant a general warrant that the Fourth Amendment prohibits?").

[350] Kerr, *Searches and Seizures*, *supra* note 340, at 569-70.

view doctrine from computer searches to avoid functionally creating general warrants.[351] So much the more on a distributed network.

Now to ownership. The *Carpenter* Court had no problem with the possibility that digital assets *can* be owned;[352] the *Carpenter* dissents instead all ruminated on the fact that Carpenter did not apparently own the specific cell-tower data in which he claimed a Fourth Amendment right.[353] Federal Rule of Criminal Procedure 41, which governs federal warrants, also defines "property" to include "information," although this still does not exactly answer how to tell whose property some given information is.[354] So, what property interest do blockchain users have in a blockchain's data, such that they could claim a Fourth Amendment interest in it under a textual reading, and by what criteria do we answer that question?[355]

At least one kind of blockchain data clearly operates as personal property in a traditional sense: cryptocurrency. Bitcoin and other cryptocurrencies, of course, strictly speaking, are nothing but intangible information, a record of exchanges.[356] But cryptocurrency is a form of personal property all the same,[357] and courts accordingly have found digital coins to be money under criminal statutes,[358] and capable of conversion.[359] Control of the private key shows ownership.[360]

But what about non-cryptocurrency data stored on chains? They can certainly be transacted. Data can also be private-key encrypted, even on an open chain, which would also indicate ownership. But once unencrypted data are put

[351] *Id.* at 566, 583.

[352] *See Carpenter*, 138 S. Ct. at 2230, 2270 (Kennedy, J., dissenting; Gorsuch, J., dissenting) (noting with approval that state courts and legislatures are developing a law of digital property).

[353] *See supra*, text accompanying note 265.

[354] Fed. R. Crim. P. 41(a)(2)(A).

[355] *See Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting).

[356] Nielsen, *Bitcoin Protocol*, *supra* note 28 ("[D]igital money is . . . just the message itself, i.e., the string of bits representing the digitally signed message 'I, Alice, am giving Bob one infocoin.'").

[357] *See generally* Joshua A.T. Fairfield, *Bitproperty*, 88 S. CALIF. L. REV. 805 (2015); Petter Hurich, *The Virtual is Real: An Argument for Characterizing Bitcoins as Private Property*, 31 BANKING & FIN. L. REV. 573, 576 (2016). *But see* Tatiana Cutts, *Bitcoin Ownership and Its Impact on Fungibility*, COINDESK (Jun. 14, 2015), https://perma.cc/2LYZ-BBT8 (arguing that for policy reasons such as reduced fungibility property law should not regulate cryptocurrencies); Bacon et al., *supra* note 26, at 193 (arguing that cryptocurrencies do not fulfil all traditional property categories).

[358] United States v. Stetkiw, No. 18-20579, 2019 WL 417404, at *2-4 (E.D. Mich. Feb. 1, 2019) (collecting cases). *But see* United States v. Petix, No. 15-CR-227A, 2016 WL 7017919, at *20 (W.D.N.Y. Dec. 1, 2016) (holding that bitcoins are not money for purposes of 18 U.S.C. § 1960, which prohibits unlicensed money transmitting businesses).

[359] *See, e.g.*, Kleiman v. Wright, No. 18-CV-80176, 2018 WL 6812914, at *16 (S.D. Fla. Dec. 27, 2018).

[360] Hurich, *supra* note 357, at 577.

on a chain, they might be copied and disseminated, which suggests lessened control.[361]

Here founding-era history can guide. Morgan Cloud has shown that in the founding era "the broad concept of property included a person's rights, ideas, beliefs, and the creative products of her labor."[362] James Madison, writing just weeks after the ratification of the Fourth Amendment,[363] shared this conception of property, listing as property a person's "free use of his faculties and free choice of the objects on which to employ them" and people's "enjoyment and communication of their opinions, in which they have an equal, and in the estimation of some, a more valuable property."[364] Madison's focus on ideas and expression as property helps explain a seeming anomaly of the Fourth Amendment's text: one's "papers" of course, are also "effects," making the Amendment redundant, unless what "papers" protect are the ideas contained in them, something that "effects" don't necessarily do.[365] As Cloud argues,

> If a person's property includes the products of his labor, then papers should be protected *as* property. And these protections were not limited to the physical paper containing a writing. The belief that the contents of papers were a person's protected property emerged as an important theme in Whig theories of liberty in the second half of the eighteenth century.[366]

Hence, if the authors of the Fourth Amendment would have considered a person's expressions, ideas, and labor, as recorded into a writing, to be property, then data that people post to blockchains should also be their property under the same framework—and the lack of *exclusive* control once posted should not be dispositive of non-property either.[367] The question might turn on whether the

[361] Fairfield, *supra* note 357, at 873.

[362] Morgan Cloud, *Property Is Privacy: Locke And Brandeis In The Twenty-First Century*, 55 AM. CRIM. L. REV. 39, 37 [hereinafter Cloud, *Property Is Privacy*]; *see also* Laura S. Underkuffler, *On Property: An Essay*, 100 YALE L.J. 127, 128-29 (1990) ("During the American Founding Era, property included not only external objects and people's relationships to them, but also all of those human rights, liberties, powers, and immunities that are important for human well-being, including: freedom of expression, freedom of conscience, freedom from bodily harm, and free and equal opportunities to use personal faculties.").

[363] Cloud, *Property Is Privacy*, *supra* note 362, at 50.

[364] James Madison, *Property, in* 6 THE WRITINGS OF JAMES MADISON 101-102 (Gaillard Hunt ed., 1906).

[365] Cloud, *Property Is Privacy*, *supra* note 362, at 55.

[366] *Id.* at 47.

[367] *See Carpenter*, 138 S. Ct. at 2269 ("I doubt that complete ownership or exclusive control of property is always a necessary condition to the assertion of a Fourth Amendment right.") (Gorsuch, J., dissenting).

person actively placed information onto a blockchain or just passively created it by carrying around a device (and if passively, the *Carpenter* majority's rule might apply instead), but the underlying principle is textual and time-honored.

Positive law will also come to help determine ownership.[368] Arizona and Tennessee have already explicitly recognized property rights in data on blockchains.[369] In February 2019 Wyoming became the first state to update its Uniform Commercial Code to recognize intangible "digital assets," the "representation of economic, proprietary or access rights that is stored in a computer readable format, and includes digital consumer assets, digital securities and virtual currency."[370] And both the state and federal courts and legislatures have also begun to recognize property interests in data communications that are informational and expressive.[371]

In all, for a textualist, blockchain data are modern-day papers containing ideas owned by the poster, or even digital personalty (currency) itself; shared, but still owned, and (at least in part) controlled. An attempt by the government to learn about those data should constitute a plain-meaning search. Such a search becomes ever more unreasonable, in historical terms, the broader its sweep; on a blockchain, a fully unrestrained search could be broad indeed. Blockchain shows how the Fourth Amendment can stay anchored in text and handle technological evolution.

2. *"Effects" and Trespass*

The question of ownership turns us to our last issue. The Fourth Amendment protects "persons, houses, papers, and effects."[372] Blockchain data may be modern-day equivalents of papers, but also may be "effects." Fourth Amendment "effects" have historically been rarely litigated and are under-analyzed,[373] but the term "effect" seems historically simply to mean "personalty," as distinct from real

[368] For the argument that positive law should inform the protections of the Fourth Amendment, see generally Baude & Stern, *supra* note 41.

[369] Ariz. Rev. Stat. § 44-7061(D) ("Notwithstanding any other law, a person that . . . uses blockchain technology to secure information that the person owns or has the right to use retains the same rights of ownership or use with respect to that information as before the person secured the information using blockchain technology."); Tenn. Code. Ann. § 47-10-202(d) (substantially the same).

[370] Wyo. Stat. Ann. § 34-29-102 (2019).

[371] *Carpenter*, 138 S. Ct. at 2270 (citing cases); *see also* Kremen v. Cohen, 337 F.3d 1024 1030 (9th Cir. 2003) (intangible internet domain name was property capable of conversion).

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

[373] Brady, *supra* note 214, at 960; Ferguson, *Smart Fourth Amendment*, *supra* note 285, at 581.

property.[374] Whether data might be effects has only been lightly explored,[375] and the Supreme Court has not yet directly taken up the question.[376] As we just saw, blockchain suggests that data are, indeed, effects.

If blockchain data are "effects," we open up a new level of analysis. Maureen Brady has argued that the "reasonable expectation of privacy" framework is inapposite to effects, which should be protected from unreasonable searches even when an effect sits unattended in public space.[377] That was also the essential holding of *United States v. Jones*, which ruled that a Fourth Amendment "search" occurs—and a warrant is required—when there is a physical trespass onto an effect (even a publicly visible effect such as a car) coupled with an attempt to gain information.[378] But what can a trespassory search to an intangible effect mean? The *Jones* majority, admittedly, seemed to imagine that a such thing is not possible.[379] With respect, there may be some thinking left to do.

Physical trespass at common law was always a legal peppercorn, a talismanic signal of a violation of some greater social value.[380] "Trespass" was also another capacious common law term, certainly signifying physical invasion, but with a broader common meaning, including an invasion into liberties.[381] Now, there was also recognition as early as *Entick* that "the eye cannot by the laws of England be

[374] Oliver v. United States, 466 U.S. 170, 177 n.7 (1984); Brady, *supra* note 214, at 986-87.

[375] Brady, *supra* note 214, at 1017; Ferguson, *Smart Fourth Amendment*, *supra* note 285, at 573-76.

[376] Debra Cassens Weiss, *Does Fourth Amendment Protect Computer Data? Scalia Says It's a Really Good Question*, ABA JOURNAL (Mar. 24, 2014), https://perma.cc/4W9X-VZWE (noting that the late Justice Scalia found the question of whether computer data are "effects" interesting).

[377] Brady, *supra* note 214, at 1012-13. *But see* Ferguson, *Smart Fourth Amendment*, *supra* note 285, at 582 (arguing for retaining "concealment" as a requirement for Fourth Amendment protection).

[378] *Jones*, 565 U.S. at 404, 408 n.5.

[379] *Id.* at 411 ("Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.") (emphasis in original).

[380] *See* Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAWYER 1395, 1429 (2007). *Jones* itself quoted *Entick v. Carrington*, (1765) 95 Eng. Rep. 807 (C.P.): "[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law."

[381] Laurent Sacharoff, *Constitutional Trespass*, 81 TENN. L. REV. 877, 892-93 (2014) ("Most generally, though perhaps archaically, [trespass] refers to committing an offense, sinning, or exceeding authorized boundaries, and the framers often used the term in this latter meaning when describing how any government tends to engross itself, enlarge its powers, and trench the people's liberties.").

guilty of a trespass."[382] But that only reminds us to be technically accurate: an investigator looking at a blockchain, to repeat, is not the same as a police officer passively accepting light particles into her eyes as she walks down a street. The former requires sitting at a computer and sending out electronic signals to other computers to obtain information about the chain.[383] If common law traditionally recognized a cause of action in the slightest touch of a foot to a blade of grass, in service of some greater societal need, it is hard to see why sending instructions to other computers should necessarily be different.[384] Indeed, some lower courts have found that "[e]lectronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action."[385]

Common and positive law, moreover, might also evolve in the face of digital assets to understand "trespass" differently from purely macro-physical touch.[386] Courts and scholars are formulating a doctrine of cyber-trespass, which currently requires some show of the traditional element of "damage" to the digital chattels.[387] But the damage requirement for cyber-trespass is so weak—as minute

[382] *Boyd*, 116 U.S. at 628 (quoting *Entick*, 95 Eng. Rep. 807). The Court has a least on one occasion, although without explanation, rejected that maxim: McDonald v. United States, 335 U.S. 451, 454 (1948) (noting government's "syllogism," that "[l]ooking over the transom was not a search, for the eye cannot commit the trespass condemned by the Fourth Amendment. Since the officers observed McDonald in the act of committing an offense, they were under a duty then and there to arrest him. . . . The arrest being valid the search incident thereto was lawful," but concluding "[w]e do not stop to examine that syllogism for flaws. Assuming its correctness, we reject the result").

[383] *See generally* Steven Li, *How Does The Internet Work?*, MEDIUM (Aug. 1, 2017), https://perma.cc/X5P6-SXR3.

[384] *See* Steven Kam, *Intel Corp. v. Hamidi: Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427, 440 ("A modern understanding of physics blurs the line between actions that qualified traditional trespass, such as bodily intrusion and bricks thrown through windows and 'intangible' invasions now understood to be 'physical,' such as particulate matter [smog, industrial fumes] and electromagnetic energy."). *But see* Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y. 1, 12-13 (2012) (calling such arguments "exotic," although with little substantive refutation).

[385] *See, e.g.*, Compuserve Inc. v. Cyber Promotions, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997); McLeodUSA Telcoms. Servs. v. Qwest Corp., 469 F. Supp. 2d 677, 703 (N.D. Iowa 2007) (permitting trespass action for electronic interference).

[386] Georgia v. Randolph, 547 U.S. 103, 144 (2006) ("There is nothing new or surprising in the proposition that our unchanging Constitution refers to other bodies of law that might themselves change.") (Scalia J., dissenting); Sacharoff, *supra* note 381, at 928 ("Courts will have to develop more fully a Fourth Amendment law of trespass"); Mannheimer, *Decentralizing*, *supra* note 216, at 187 ("What we know as trespass is simply the fully formed product of that evolutionary process. That evolutionary process continues to this day.").

[387] Shyamkrishna Balganesh, *Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass*, 12 MICH. TECH. L. REV. 265 (2006); Richard A. Epstein,

as temporarily slowing down a plaintiff's server—that some commentators see trespass to digital chattels as practically equivalent to damage-less action for trespass to land, actionable upon a very slight interference with the data.[388] Indeed, several courts and scholars have concluded that the mere copying of electronic data constitutes a Fourth Amendment *seizure*, classically an interference with a "possessory interest."[389]

No doubt, caution is again due: "We cannot know whether [the framers] would have extended the general principle against unreasonable trespassory invasions to nontrespassory invasions."[390] But in all, blockchain so closely mimics a common-law "effect," with all of the rights that traditionally pertain to "effects," that to declare that such an effect can never suffer a trespass-search would create an unnecessary anomaly, and might well be "bad physics as well as bad law."[391]

IV. A WAY FORWARD: OPEN DISTRIBUTION, SECURITY, AND CONTROL

I have proposed that the Fourth Amendment can restrict government examination in criminal investigations of technologically advanced but open, shared, and distributed information. That is hard to imagine because blockchain is so conceptually difficult; because we are used to the inside/outside, content/non-content, and third-party rules; and because we are used to living in a physical world where "public" and "private" are easily distinguished. For half a century, "privacy" has been the on-off switch for Fourth Amendment protection because it is the on-off switch for many fundamental human activities in the physical world. With privacy, certain freedoms are exercised or activities undertaken; without it, they are not. But privacy may no longer be such an on-off

Cybertrespass, 70 U. CHICAGO L. REV. 73 (2003) [hereinafter Epstein, *Cybertrespass*]; Richard A. Epstein, *Intel v. Hamidi: The Role of Self-help in Cyberspace?*, 1 J.L. ECON. & POL. 147 (2005); Daniel Kearney, *Network Effects and the Emerging Doctrine of Cybertrespass*, 23 YALE L. & POL'Y REV. 313 (2005); Richard Warner, *Virtual Borders: Trespass to Chattels on the Internet*, 47 VILL. L. REV. 117 (2002). A much of this debate centers on interpreting the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, and on the extent to which an allegedly unauthorized access to a computer might be a "trespass." Roughly, the argument goes, indicia of violation of computing "norms" or attempts to retain some control of data would signal that unauthorized access to those data is a trespass; indicia of relinquished control freely to the general public signals there can be no trespass to the data. *See, e.g.*, Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1146-47 (2016); Winn, *supra* note 380, at 1428.

[388] Balganesh, *supra* note 387, at 284 (noting that the weakened damage requirement is "effectively rendering the requirements of cybertrespass analogous to those of trespass to land"); Esptein, *Cybertrespass*, *supra* note 387, at 83 (noting that in many ways "cyberspace looks and functions more like real property than chattels").

[389] Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 372-73 (2015).

[390] Wasserstrom & Seidman, *supra* note 157, at 78.

[391] *Katz*, 389 U.S. at 362 (Harlan, J., concurring).

switch. Things formerly protected by privacy are now protected by openness, distribution, and mathematics. So now what?

One possible response is to throw blockchain into *Katz*'s framework and live with the outcome: respect for an individual's private key and home computer and unrestricted searches of all other blockchain data of countless people, without any discernible limit, forever, even as the technology expands into the mainstream. Many would disagree with that imbalanced outcome, especially given that the reasonable-expectation-of-privacy test and privacy-as-secrecy are under attack from scholars and the Justices themselves, and particularly in light of ever-more-ubiquitous technology.

Another alternative is to zero in on another principle for the Fourth Amendment to uphold. Options include security from government intrusion, freedom of expression, and personal autonomy. As a philosophy enacted into a technology, blockchain shares these interests with the Fourth Amendment, and shows how to achieve these ends without secrecy—an open, shared, digital architecture that provides its users control over their data.

A third alternative is to return to the Amendment's text and determine whether a search, in the ordinary meaning of the term, occurred of defendant's digital analogue to a paper or effect, and whether that search was "reasonable" as the Fourth Amendment understands that word. That test hearkens back to broad conceptions of rights and personhood as expressed through property and the fear of wide-reaching indiscriminate searches; blockchain shares those ideals and provides a model for how to carry text and history intact into twenty-first century technology.

In the absence of on-point legislation, these latter two alternatives are preferable. Given the Court's current composition, it might come to adopt the textual framework as described above in Part III.E. But we also need to subject these approaches to "principled application."[392] And the third, textual framework might be too rigid for blockchain, especially if it requires a full-on warrant every time investigators seek to look at chains.

I propose a more flexible framework for investigations into blockchain data. The key distinction through which to analyze blockchain data in this new framework would not be public/private, or content/non-content—distinctions hollowed out by blockchain's openness and distribution—but rather *controlled/semi-controlled/relinquished*. We have repeatedly seen how blockchain's openness and distribution provide a person with a level of control over data that privacy no longer provides. That control underpins the security, expression, and property values that the Fourth Amendment vindicates. The proposed distinction, that is, would do the work within blockchain's digital space that

[392] *See* Slobogin, *A Defense of Privacy*, *supra* note 158, at 148.

traditional distinctions that turn on privacy once performed for the physical world.

A judge's first step in this framework would be to determine the level of control. A user's true identity and private key strings would easily be classified as fully controlled information, relinquished to no one. Encrypted data on public chains would also evince full control. Data posted to a blockchain to ensure security and to prevent damage, theft, or loss would be considered semi-controlled; a clear interest in their not being damaged or manipulated has been retained in them, even if they have been posted to an open chain. Other indicia of semi-control might be distribution restrictions on data posted to chains. Data held by consortia on permissionless chains would be considered fully controlled as to companies that create and keep them. As for the individuals who created the data by living their lives with a device, they should by default retain a semi-controlled interest in the integrity of their personal data on a private chain, absent clear indicia that the individuals purposely relinquished the data for general public viewing.[393] By contrast, truly public data on a blockchain, clearly released for public consumption (that is, not merely to gain the advantages of secured transaction) would be considered relinquished.

The controlled/semi-controlled/relinquished distinction is implicit in the Fourth Amendment's text, in the ownership and control that the people exercise in "their" persons, houses, papers, and effects, and in their right to be "secure" in that control against unreasonable government interference therein. Further, the distinction can be applied without any special reference to any atextual and muddled privacy or secrecy concepts, or the circularity of *Katz*'s "expectations." It also stands as a logical extension of the Supreme Court's recent cases that shift doctrine in the face of technology. It recognizes, as the *Carpenter* majority did, that technology makes qualitative differences in how we assess longstanding doctrine, and that some Fourth Amendment protection for public acts is now not only conceivable, but critical to prevent government overreach. It participates in the *Jones* "effects" framework and the *Carpenter* minority's focus on ownership, and it also acknowledges that the digital world has counterintuitive gradations in how control is digitally exercised and shared. The distinction also undergirds the values that scholars have argued that the Fourth Amendment defends: security, autonomy, self-direction, and the free choice of self-expression. Although there would be some room for judgment in its application,[394] the distinction is also a

[393] The data of such individuals might also be governed by *Carpenter's* majority holding, depending on the pervasiveness of the data collection. *See supra*, text accompanying notes 289-90.

[394] The technical details of chains can vary, for instance, making the question of control, semi-control, or general relinquishment harder to assess. I trust, however, that judges can be guided by the underlying principles and touchstones: has the person decided to share

fairly clear trigger, providing less opportunity for the naked policymaking that the malleable concept of "privacy" begets. It especially creates a clear line against the Fourth Amendment's principal bogeyman: the general warrant. Information clearly relinquished for public use would never have required a warrant at common law, and would not require one now. Inclusion of data on a blockchain for the sake of security and control, however, is blockchain's substitution for privacy, and indicates that the government has not been invited for an eternal look around at its leisure.

A judge's next step would be to apply a level of restraint. Blockchains are going to contain critical criminal evidence, and we must balance law enforcement's legitimate need for that evidence with civil liberties, and without minting complex new rules for law enforcement or making it prohibitively difficult for law enforcement to access information. Luckily, there exists a familiar ladder of Fourth Amendment justifications for intrusion that correspond to the three possible distinctions.

Police review of purely relinquished blockchain information would require no judicial oversight, ex ante or ex post, just like items currently in plain view, and the data would receive no special Fourth Amendment protection merely because they were posted on a chain (except inasmuch as police investigation into the material raises traditional First Amendment censorship or chilling concerns exacerbated by an immutable ledger).[395]

Semi-controlled information, however, should be regulated by a novel application of the "reasonable suspicion" standard, itself a recognition that the Fourth Amendment is not an on-off switch but admits workable gradations that balance the "reasonableness" of government intrusion with the people's rights, and that already works for another technology that straddles public, open, controlled, and private axes—the automobile.[396] Judicial oversight for examinations of semi-controlled data would not be necessary *ex ante*, to free law enforcement to investigate crime reasonably efficiently. But officers would *ex post* need to articulate a reasonable suspicion of why they wished to review semi-controlled data, and would have to show how their efforts were limited to the issue and suspect at hand and did not bleed into a full-blown study of the whole chain. One could imagine, for instance, law enforcement narrowing in on a suspect, and, acting on an articulable suspicion that he might be engaging in cryptocurrency transactions for goods in certain amounts at certain times,

completely, guardedly, or not at all with the world, and would unfettered government investigation of the information amount to a general warrant?

[395] As described in *supra* Part III.D.iii.

[396] South Dakota v. Opperman, 428 U.S. 364, 368 (1976) (noting that automobiles are not subject to the full warrant requirement but are subject to a reasonable suspicion stop, in part because a car travels "public thoroughfares where both its occupants and its contents are in plain view").

reviewing a chain in a targeted way for specific clues.[397] What the standard would not permit are large-scale scans resembling mass surveillance or pure fishing expeditions on hunches alone. It would be quite easy to know when the standard is triggered: law enforcement would have to articulate some reasonable suspicion why it was looking for the semi-controlled data before it logged on to review a chain.[398]

Finally, fully controlled information would require a full warrant supported by probable cause. That, as mentioned, would specifically include a warrant before law enforcement began attempting to de-anonymize hidden identities, which require massive, expert sweeps.[399] Probable cause could, naturally, arise from information that the officers learned during a "reasonable suspicion"-style search of semi-controlled data, which they could then use to apply for a warrant. Warrants would all the same have to be crafted carefully to avoid rooting out the blockchain data of thousands of people indiscriminately. This standard would therefore strike a reasonable balance in a new digital context among the need for society to deter crime, the reality that blockchains pose a challenge for criminal investigation, the people's interests in their data, and the fear of general warrants and mass surveillance.[400]

In my recommendations, I am attempting to not "embarrass the future."[401] Blockchain technology is moving quickly. It is already said to have changed from version 1.0, currency, to 2.0, smart contracts, to 3.0, distributed applications, to 4.0, enterprise uses.[402] There will be many unanswered questions to address. Accordingly, I have focused on analyzing blockchain's foundational architectural features, which are likely to be the most durable aspects of the technology. The

[397] *See* Steven Goldfeder et al., *When the Cookie Meets the Blockchain: Privacy Risks of Web Payments Via Cryptocurrencies* (2017) (explaining how third party web trackers can supply sufficient information to identify purchasers of goods from online merchants using bitcoins, absent certain precautions).

[398] One counter-argument that it is impossible to know ex ante whether a bit of blockchain data is fully relinquished or semi- or fully controlled before the examination. *See* Kerr, *Searches and Seizures*, *supra* note 340, at 545. On a blockchain it is not very difficult to guess, however, because most chains will by default be semi-controlled, and open-information sharing platforms will almost certainly advertise that fact. Edge cases might come under a good faith or other traditional exception.

[399] *Supra*, text accompanying note 201.

[400] I take a cue from Orin Kerr in attempting to readjust the status quo ante equilibrium between police and technology users as technology grows more powerful. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

[401] *Carpenter*, 138 S. Ct. at 2220 (quoting Northwest Airlines v. Minnesota, 322 U.S. 292, 300 (1944); *see also* Kerr, *Applying the Fourth Amendment*, *supra* note 215, at 1038 ("When technology is new, social understandings remain contingent: we might initially misunderstand the new technology and misconstrue or diverge on its privacy implications.").

[402] Unibright.io, *Blockchain Evolution: From 1.0 to 4.0*, MEDIUM (Jan. 14, 2019), https://perma.cc/4HSK-3UZK.

framework I propose is therefore flexible, reasonably familiar to courts, and corresponds to those general architectural features and the purposes they serve. But details will vary from chain to chain, and may make an analytical difference in a given case.

All the same, I want to invoke the old maxim, *obsta principiis*.[403] If the Fourth Amendment is too *slow* to move in the face of technological change, violations of the Amendment can gain the force of custom, and then be difficult to dislodge. Now is the time to start to consider how to handle this new technological landscape. Cases will be coming, and soon. Doctrine will have to either double down, or shift. The shift can begin by recognizing that Fourth Amendment doctrine cannot truly handle this new technology and remain a bulwark against government intrusion if the purpose of the Fourth Amendment is to protect "privacy-as-secrecy." Distributed ledgers should instead catalyze a developed Fourth Amendment jurisprudence that focuses on text, history, security, autonomy and control, and defense against the accumulation of Leviathan's power.[404]

[403] *Boyd*, 116 U.S. at 635.

[404] Donohue, *supra* note 24, at 685 ("By acknowledging that the purpose of the Fourth Amendment was to protect against the accumulation of power, the Court will be better equipped to confront the dangers of the digital age.").