The Judges' Book

Volume 5 Article 8

2021

Constitutional Law: Blockchain's Challenge for the Fourth Amendment

Paul Belonick

Constitutional Law

Blockchain's Challenge for the Fourth Amendment

Paul Belonick[1]

Introduction

Blockchain technology is now hitting the mainstream. Digital currencies based on blockchain architecture, such as Bitcoin and Ethereum, are growing in acceptance, and major corporations are using blockchains to store troves of data from their devices, supply chains, and services. But what is a "blockchain?" And what, if anything, does the Fourth Amendment have to do with it? This Chapter answers those questions for lawyers, scholars, and judges.

How Does It Work?

Blockchain (or "distributed ledger technology") is a digital architecture for a community of users to keep data on an open, shared, and highly tamper-resistant common ledger.[2] Blockchains can both store information and create mediums of exchange, such as digital "coins" transferrable over the ledger. The central purpose of blockchain is to store and exchange data while making tampering and fraud all but impossible—but in a new, revolutionary way. In the physical world, information and valuables are secured through exclusion and secrecy: guarded

---

[1] Excerpted and adapted from Paul Belonick, *Transparency is the New Privacy: Blockchain's Challenge for the Fourth Amendment*, 23 STAN. TECH. L. REV. 114 (2020).

[2] Good resources on blockchain include Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, *Blockchain Demystified: A technical and legal introduction to distributed and centralised ledgers*, 25 RICH. J.L. & TECH. 21 (2018); Michael Nielsen, *How the Bitcoin Protocol Actually Works*, DATA DRIVEN INTELLIGENCE (Dec. 6, 2013); Regional Organized Crime Information Center, *Bitcoin and Cryptocurrencies, Law Enforcement Investigative Guide* 6–7 (2018) [ROCIC Report]; KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 91 (2018); Dylan J. Yaga, Peter M. Mell, Nik Roby & Karen Scarfone, *Blockchain Technology Overview*, NISTIR 8202 iv (Oct. 2018).

repositories, secured servers, passwords, locks, etc. Blockchain's radical insight is that in the right digital circumstances, things shared and seen among a network of anonymous strangers can be more secure from alteration and censorship than things kept private and hidden.

Five main features of blockchain's open, shared architecture create this novel level of security.[3] First, the ledger is kept across numerous computers and is updated simultaneously, creating multiple backups.

Second, the integrity of the ledger is protected not by a private reconciliation agent like a bank but by a process of sharing. Parties who want to exchange data on the ledger propose their transactions to "validating" computers on the network, which earn the right to publish the exchange on the ledger by solving complex mathematical problems that require immense computing power.[4] Once the validator wins the right to publish, it is rewarded for validating proper transactions with "coins" or other incentives. But if the validator attempts to publish improper or fraudulent transactions, the community of computers—which can review all accounts on the open ledger—rejects the validation, to the great lost energy and time of the validator.

Third, the data, when exchanged, are digitally scrambled ("h-ashed") by algorithmic formulas called "keys" into randomized strings of characters called "digests," which can be unscrambled only by someone with a paired key. Decoding the digests without the keys by trial and error would take *billions* of years, even for powerful supercomputers.[5] Digests make data tampering evident: a change of one character in even massive amounts of underlying data generates a visibly different digest when hashed. Thus, while final transactions on a blockchain are published uncoded on the ledger, keys and digests make data hacking and fraud in transit all but impossible.

---

[3] These are general features; different blockchain protocols vary in detail. ROCIC Report, *supra* note 2, at 7.

[4] In some blockchain architectures, the validator has to "stake" some cryptocurrency to win the right to publish. WERBACH, *supra* note 2, at 57. The point is the same: to force the validator to take a serious risk of loss if the other network members reject the proposed transaction.

[5] Patrick Nohe, *What is 256-bit Encryption? How Safe is It?*, HASHEDOUT (May 2, 2019).

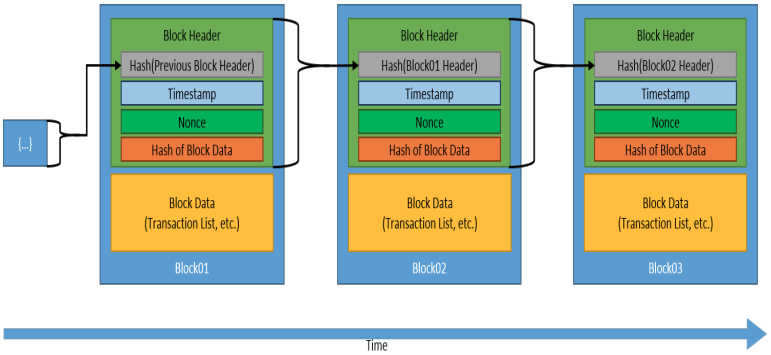
Fourth, blockchains use traditional privacy in a unique way. Blockchain users have two keys: a public key shared with others, and a private key known only to an individual user that alone can unscramble digests created by the user's public key. Owners of data identify themselves on a blockchain by anonymous digital "addresses" associated with their public key and their data on the ledger. Dual keys and addresses create data security even among anonymous strangers: counterparties "sign" proposed transactions by showing that they can unscramble test data scrambled by their public keys, which shows that they are the true owners of the data on the ledger associated with their digital addresses. Anyone can read the data being exchanged among parties on the ledger, but perfect strangers can be assured that their anonymous counterparties indeed own what the open ledger says they do, while everyone's real-world identity can remain hidden.[6]

Fifth, openness and distribution—as opposed to secrecy and exclusion—create blockchain's data security. Validating computers layer proposed transactions into algorithmic "chains" of "blocks" (ledger entries) of data. Each block has two parts: the stored ledger data within the block (the "payload"), and the "header," a digest that identifies the block. The header is derived from hashing together the data in the payload, some identifying data, proof of solving the complex puzzle, and the header of the *previous* block, which was created in the same way using the header of *its* predecessor, and so on backwards. A block's header is thus rooted mathematically in every previous block of data, and then roots the header of every later block.

Once a validating computer proposes to publish a block, other computers on the network review the block and can "accept" it by hashing the next proposed block to it and updating the rest of the network on the "shared state" of the ledger. Hence, the network collectively builds a chain of blocks mathematically connected by header digests:[7]

---

[6] ROCIC Report, *supra* note 2, at 3; Yaga et al., *supra* note 2, at 11.
[7] Image from Yaga et al., *supra* note 2, at 17.



The upshot is that once network consensus joins a block to the ledger chain, any change to the block's payload, even a single character, will automatically algorithmically change the header digest of its block radically, creating a ripple effect in all the linked headers down the chain.[8]

Every computer viewing the open copy of the ledger could observe that effect.[9] Distribution and openness thus make blockchain data "tamper evident." More so, distribution and openness make the chain "tamper resistant": the *only* way to alter a block's data once it is on the ledger chain is to try to "republish" it and then "revalidate" every following block in sequence from the altered block up to the present.[10] But that would require impossibly phenomenal (and exponentially increasing) amounts of computing power to solve those complex validation puzzles in time to beat out all the legitimate blocks that other validators are adding to the end of the ledger chain—all to no avail once the changes are detected and rejected by the group consensus anyway.[11] The one sure way to get away with fraud or censorship is to own 51% of the computing power of the network so that one could self-validate any transaction and repeatedly hash blocks on top of it ahead of other validators no matter who objected. But that

---

[8] *Id.*

[9] *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." Peter Hurich, *The Virtual is Real: An Argument for Characterizing Bitcoins as Private Property*, 31 BANKING & FIN. L. REV. 573, 577 (2016).

[10] Bacon et al., *supra* note 2, at 17.

[11] Nielsen, *supra* note 2.

feat becomes computationally unattainable once a blockchain network gets large enough.[12]

Hence, blockchain data records are, for all intents and purposes, immutable. All users can see data on the ledger but—in part for that very reason—can't do anything to change them, steal them, censor them, or to dupe others into accepting fraudulent offers of them. No central reconciliation mechanisms or costly fraud protections are needed. Mathematical laws and visibility to a large community of computers together create "structured transparency" that secures against fraud and manipulation to an extent that other computing methods or physical world means based on secrecy and exclusion cannot match. The technology is amazingly powerful: In a test to discover which farm had supplied Wal-Mart a particular package of mangoes, conventional tracking mechanisms identified the supplier within a week; blockchain took two seconds.[13] For this reason, blockchain enthusiasts (perhaps a bit too animatedly) claim that blockchains will create frictionless exchanges of information and value that will transform economies, governments, and perhaps all human relations.[14]

But there is a downside to security by transparency: with the growth of blockchains as widely used personal payment and enterprise data-management tools, millions of everyday actions and transactions will be recorded permanently, leaving digital traces of people's interactions on ledgers that are immutable and—to varying degrees—visible. Mass surveillance will never have been easier.

Blockchain and the Fourth Amendment

How should Fourth Amendment caselaw react? I propose engaging blockchain thoughtfully, considering first how some settled Fourth Amendment doctrines might apply to blockchain's

---

[12] Several hundred of the world's fastest supercomputers *combined* could not manage this feat in the Bitcoin network. Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 513–14 (2018).

[13] WERBACH, *supra* note 2, at 83.

[14] *Id.* at 91.

features.[15] For instance, many blockchain users likely harbor reasonable expectations of privacy in keeping their identities cryptographically shrouded[16] and in keeping their private keys—which often enough are stored in private computers in digital folders called "wallets"—private.[17] Current doctrine thus might be adequate for criminal investigations seeking to search a suspect's computer for their private key to match them to transactions, or for investigations that use complex computing systems not in general public use to try to deanonymize users.[18]

Yet, in large part because of the mass-surveillance problem, blockchain also forces a reckoning with current Fourth Amendment caselaw's shortcomings. Courts should start by recognizing that Fourth Amendment jurisprudence historically has depended on proxies—such as property and privacy—to uphold the textual right to be "secure" from unreasonable government intrusion. Technology has repeatedly forced those proxies to shift; as new investigative tools expanded the invasive powers of the government over the past century, for instance, Fourth Amendment jurisprudence changed focus from a property-based "trespass theory" to the current "reasonable expectation of privacy" theory covering everything from tapped phone conversations[19] to the "whole of one's physical movements" in space as tracked by one's cell phone.[20] Further shifts are expected as the reasonable-expectation-of-privacy test has become subject to biting criticism as confusing, subjective, and atextual, and (as

---

[15] Caselaw is as yet rare. *But see* United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020) (holding that the defendant lacked a reasonable expectation of privacy in blockchain data).

[16] Notably, regulators have proposed deanonymization for certain blockchain transactions. *See, e.g.*, 85 Fed. Reg. 83,840 (Dec. 23, 2020).

[17] ROCIC Report, *supra* note 2, at 15.

[18] *See* Raymond Shih Ray 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."). People who willingly expose their identities or who are readily identifiable with methods currently available to law enforcement would, of course, fall under current doctrine.

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

[20] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

technology becomes more searching and total "privacy" becomes ever more impossible) apt to turn the Fourth Amendment into a "dead letter."[21] The Supreme Court's latest pronouncements in such cases as *Carpenter v. United States*[22] and *Riley v. California*[23] especially portend change as technology further advances; several justices now focus directly on government overreach and are ready to abandon the privacy proxy. It appears time to move on.

Blockchain's revolutionary architecture may prove the vehicle for this next shift. To start, blockchain starkly exposes some of the illogic of the "privacy" regime. In particular, it challenges the third-party doctrine, which declares that an (atextual) reasonable expectation of privacy (and thus Fourth Amendment protection) is lost in *anything* shared with another person, making "privacy" tantamount to total *secrecy*. In the physical world, this proxy makes tolerable sense: historians have shown that the desire for security against government intrusion that inspired the Fourth Amendment was commensurate with the desire for security against private parties' trespasses on private property that resulted in damage or unauthorized use.[24] It follows that efforts to keep something "secure" against neighbors should apply equally to the government,[25] and, in the physical world, that naturally means *hiding* things we want kept safe. In the digital world, however, total secrecy is quickly growing unrealistic.

Because most blockchain data are shared on an open network, they would seemingly lose all Fourth Amendment protection

---

[21] *See, e.g.*, Paul Ohm, *The Fourth Amendment in A World Without Privacy*, 81 MISS. L.J. 1309, 1320 (2012).

[22] 138 S. Ct. 2206 (2018).

[23] 573 U.S. 373 (2014).

[24] Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 951–52 & n.13, 987–94 (2016). Brady's point makes good historical sense: regular police forces did not exist in the 18th century, and fellow citizens were the main investigators and enforcers of public order. William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 424 (1995).

[25] Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 110 (2008) ("[T]hat which we have exposed to perfect strangers, we cannot claim to be private. . . . To the extent we have opened something otherwise private to a perfect stranger, the police may intrude into it as well.").

under the third-party doctrine. Yet courts should not react in a knee-jerk manner. To start, blockchain's mind-bending architecture confounds Fourth Amendment doctrine's basic private/public, inside/outside logic: is the digital address, for instance, unprotected "non-content" like a physical address on a letter, or protected "content" like the inside of a letter in that it communicates the critical facts that the user is legitimate and an offer authentic? Is the visible data payload like the "inside" of an envelope and the anonymous address like the "outside," or the reverse? Standard physical-world analogies and the doctrines they support collapse in this novel digital space.

The third-party doctrine is already extremely unpopular, especially among the current justices. *Carpenter* leaves the doctrine on "life support,"[26] holding that the doctrine does not apply to data taken from "indispensable" modern devices or to "comprehensive" records of one's movements. *Carpenter* has direct implications for blockchain: blockchain is approaching indispensable and ubiquitous status as more businesses and people adopt it. And the comprehensive nature of blockchain data taken from, say, self-driving cars or the internet-of-things may give the Court pause. Indeed, *Carpenter* insisted that the Fourth Amendment "take account of more sophisticated systems that are already in use or in development."[27] Most pressingly, *Carpenter* goes beyond mere proxies to focus directly on "basic Fourth Amendment concerns about arbitrary government power."[28] Clinging to the third-party doctrine in the face of growing blockchain use would run afoul of the Court's warnings, permitting governments to inspect at whim blockchain records for decades' worth of information about people's daily lives.

Blockchain forces consideration of whether privacy and secrecy might, like the property proxy of old, be *incomplete* proxies for other vital human ends, including both security from intrusion protected by the Fourth Amendment and free-speech and free-association rights protected by the First Amendment. Censorship resistance and free information flow are a large part of blockchain's *raison d'être*.[29] Chinese citizens, for instance, are

---

[26] *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).
[27] *Id*. at 2218 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).
[28] *Id.* at 2222.
[29] WERBACH, *supra* note 2, at 158.

using Ethereum-based blockchains to circumvent government expurgation of the news.[30] Blockchain's immutable ledger and cryptographic anonymity can help keep speech robust and open by being both sharable and resistant to censorship, fulfilling a critical human end without relying on total privacy. Blockchain also increases personal autonomy—what Justice Brandeis once called the "right to be let alone"[31]—by reducing reliance on external actors like banks and governments. But blockchain serves these vital ends by abandoning, not by relying on, Fourth Amendment-style privacy and secrecy.

Because the goals formerly protected by secrecy can now, though blockchain, be protected by openness, distribution, and mathematics, doctrine must shift again. A new paradigm can ensure that blockchain data tied to personal autonomy enjoy Fourth Amendment security against unreasonable searches, even for shared or public data.

The new paradigm should focus on the individual's level of control over the subject of the search. Under this schema, a user's true identity and private keys would be classified as fully controlled information, relinquished to no one, and would have full Fourth Amendment protection. Data held by private consortia would be considered fully controlled as to those that keep them. Data posted to a blockchain to ensure security and to prevent damage, theft, or loss would be considered semi-controlled because of a clear interest in their integrity and security, even if they have been posted to an open chain. Individuals who create data by living their lives with a blockchain-associated device should by default retain a semi-controlled interest in the integrity of their personal data, absent clear indicia that the individuals purposely relinquished the data for general public consumption. By contrast, truly public data on a blockchain, clearly released for public consumption (that is, not put on the chain merely to gain

---

[30] Nir Kshetri, *Chinese internet users turn to the blockchain to fight against government censorship*, THECONVERSATION.COM (Feb. 25, 2019). 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). The denouement remains to be seen.

[31] Olmstead v. United States, 277 U.S. 438, 478 (1927) (Brandeis, J., dissenting).

the advantages of secured transaction) would be considered relinquished.

Data with the lowest level of control—publicly relinquished blockchain data—should have no Fourth Amendment protection. Semi-controlled data should be subject to the "reasonable suspicion" standard. Fully controlled data would require full Fourth Amendment protection of probable cause and a warrant. These distinctions based on level of control are implicit in the Fourth Amendment's textual promise to the people of their right to be secure in "their" persons, houses, papers, and effects. Further, the distinction can be applied without reference to atextual and abstract notions of privacy or secrecy or to the circularity of *Katz*'s "expectations."[32]

What the schema would *not* permit would be large-scale scans, mass surveillance, or pure fishing expeditions into ledger data based on hunches alone. Government officials therefore could not cast a dragnet over semi-controlled data at their pleasure; they would need to articulate some clear reason for analyzing the data and for focusing on any given individual. For instance, law enforcement might narrow in on a suspect, and, acting on an articulable suspicion that the suspect might be engaging in cryptocurrency transactions for goods in certain amounts at certain times, review a chain in a targeted way for specific clues.

Ironically, this approach to the 21st century's latest technology shows how the 18th-century text's focus on ownership, control, and fear of general warrants may be a better means to achieving "security" against the government than privacy-as-secrecy. Textualists, including some current justices, have suggested scotching the atextual reasonable-expectation-of-privacy test in favor of a simpler test in which a defendant's records are protected from searches that are unreasonable to the extent that they resemble the old general warrants or writs of assistance that permitted the king to search as he wished. Perusal of an open, immutable blockchain similarly could instantly reveal years of activities, edging closer to "near perfect surveillance."[33]

---

[32] Police investigation into the public material might, of course, raise traditional First Amendment censorship or chilling concerns exacerbated by the immutable ledger.

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

This view can work with my proposal: a bit of blockchain data is a modern-day paper owned and at least partially controlled by its creator. An attempt by the government to learn about those data should constitute a plain-meaning search. Such a search becomes more unreasonable, in historical terms, the broader its sweep is. On a blockchain, an unrestrained search of controlled or semi-controlled data could be broad indeed. Blockchain shows how the Fourth Amendment can stay anchored in text and handle technological evolution.

Conclusion

In sum, the proposed standard would advance judicial and scholarly critiques of current doctrine, be rooted in the Fourth Amendment's text and history, and 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. Distributed ledgers should catalyze a developed Fourth Amendment jurisprudence that eschews proxies and focuses on text, history, security, autonomy, control, and defense against the accumulation of overweening government power.

* * *