No. 23-1565

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

JAMES HARPER,

Plaintiff-Appellant,

v.

DANIEL I. WERFEL, in his official capacity as Commissioner of the Internal Revenue Service; INTERNAL REVENUE SERVICE; JOHN DOE IRS AGENTS 1-10,

Defendants-Appellees.

On Appeal from the United States District Court for the District of New Hampshire
Case No. 1:20-cv-00771 (Laplante, J.)

BRIEF OF PARADIGM OPERATIONS LP AS *AMICUS CURIAE* IN SUPPORT OF APPELLANT AND REVERSAL

Rodrigo Seira
PARADIGM OPERATIONS LP
548 Market Street
San Francisco, CA 94104
Tel.: (415) 986-9283

Omer Tene
Christopher J.C. Herbert
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, MA 02210
Tel.: (617) 570-1000

Andrew Kim
Gabe Maldoff
GOODWIN PROCTER LLP
1900 N Street, N.W.
Washington, D.C. 20036-1612
Tel.: (202) 346-4000
andrewkim@goodwinlaw.com

Counsel for Amicus Curiae
Paradigm Operations LP

Dated: October 20, 2023

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Paradigm Operations LP states that it has no parent corporation and that no publicly traded corporation owns 10% or more of its stock.

/s/ Andrew Kim
Andrew Kim
GOODWIN PROCTER LLP
1900 N Street, N.W.
Washington, D.C. 20036-1612
Tel.: (202) 346-4000
andrewkim@goodwinlaw.com

Counsel for Amicus Curiae
Paradigm Operations LP

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

Paradigm Operations LP ("Paradigm") is a research-driven investment firm that focuses on crypto and related technologies at the frontier. Paradigm takes a hands-on approach to help projects reach their full potential, from the technical (mechanism design, security, engineering) to the operational (recruiting, go-to-market, legal and regulatory strategy).

Crypto and the blockchain technology that powers it are new computational frameworks that have the potential to democratize the internet and revamp many sectors of the economy, including the global financial system. Despite their nascency, crypto and blockchain technology will play an essential role in everyday life. One in five Americans have interacted with crypto in some way, with the number of blockchain participants skyrocketing over the years; indeed, as of October 11, 2023, there were over 246 million unique addresses interacting on the Ethereum blockchain.[2] Blockchain technology could eventually be used for ordinary,

[1] All parties have consented to the filing of this amicus brief. No counsel for any party authored this brief in whole or in part, and no party, counsel, or person other than *amicus curiae* and its counsel contributed money to fund the preparation or submission of this brief.

[2] *See* Joanna Ossinger, *The World's Cryptocurrency is Now Worth More Than $3 Trillion*, Time (Nov. 8, 2021, 8:23 PM), https://time.com/6115300/cryptocurrency-value-3-trillion; Commissioner Jaime Lizarraga, *Digital Assets: Putting Investors First*, SEC (Nov. 16, 2022), https://www.sec.gov/news/speech/lizarraga-brooklyn-law-school-20221116; *see also Ethereum Unique Addresses Chart*, Etherscan (last visited Oct. 11, 2023), https://etherscan.io/chart/address.

everyday affairs—a trip to the store, a visit to the doctor, or voting in an election. Paradigm firmly believes in the promise and potential that crypto and blockchain technology will deliver.

The district court's decision threatens to curtail that promise and potential. In concluding that there is no expectation of privacy when a person transacts on a crypto exchange, the district court failed to give weight to the inherent expectation of privacy that forms an essential part of the foundation of crypto and blockchain technology. As a leading supporter of, and investor in, crypto and other blockchain-related projects, Paradigm has a strong interest in ensuring that Fourth Amendment caselaw recognizes the critical role that privacy plays with respect to this emerging technology.

INTRODUCTION

Crypto asset transactions are powered by blockchain technology, which leverages decentralized protocols that distribute operations across a network of computers or nodes. In these decentralized systems, information that would ordinarily be in the custody and control of a single clearinghouse (like a bank, or a government agency) is distributed across a network that is responsible for maintaining the accuracy and integrity of the "ledger."

As suggested by the prefix "crypto"—derived from the concept of computer cryptography—privacy is a foundational pillar of crypto transactions, a pillar

reinforced by the decentralized network architecture. Certain aspects of crypto transactions—the date and time a transaction took place, and the amount of a transaction—may be publicly viewable on the ledger. But crypto pseudonymizes the participants of a transaction—the only "identity" revealed is a long, alphanumeric string of hexadecimal characters called a public key or "wallet." There are many valid reasons why crypto users want to maintain the ultimate ownership of a wallet private—a user may, for example, want to keep hidden his or her participation in social movements, such as support for Ukraine's defense against Russian aggression.

Despite the district court's conclusions to the contrary, crypto has an inherent expectation of privacy; that expectation does not evaporate simply because a user chooses to transact through a centralized exchange, rather than through the blockchain itself. The court reasoned that a crypto transaction on an exchange is like a bank transaction—neither purportedly gives rise to an expectation of privacy because, in both scenarios, information about the transaction and its participants is handed to a third party. But the very nature and design of crypto gives rise to a more substantial expectation of privacy than that of bank records and negotiable instruments, which are often passed between intermediaries with full identifying information in view. And, as the Supreme Court clarified in *Carpenter v. United*

States, 138 S. Ct. 2206(2018), a person does not surrender his or her expectation of privacy merely by public exposure.

Moreover, the district court failed to account for the nature of the Government's intrusion here. The underlying lawsuit arises from a so-called John Doe summons, which is intended to allow the IRS to investigate a *specific* taxpayer (or a group of taxpayers) whose identity is not known to the IRS. But the IRS's summons here was not specific at all; rather, it was akin to a fishing net, designed to collect a broad swath of information on more than 10,000 users, in which the plaintiff, James Harper, happened to get caught. As Congress recognized when it enacted the statute authorizing John Doe summonses, the privacy intrusion is different—and more severe—when an agency uses its subpoena power to conduct a fishing expedition. Even assuming it is reasonable for a person to expect that law enforcement officials might go to a third party and ask for specific information about that third person's account, the reasonable person would never expect that his or her information would be dumped out as part of a treasure trove of records for a government agency to dig through. The Fourth Amendment does not allow the Government to go fish; indeed, "it was … the use of" broad and indiscriminate "general warrants and … writs of assistance that led to the ratification of the Fourth Amendment" in the first place. *See United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 327 (1972).

For these reasons, this Court should reverse the district court's decision as it relates to Harper's Fourth Amendment claim.

ARGUMENT

I. Blockchain technology is designed to improve transparency and to protect the integrity of information, while returning some measure of control over the disclosure of information to end users.

At its core, the blockchain technology that powers crypto allows for distributed processing of data, such that no single, central authority is responsible for maintaining and preserving records. *See* Paul Belonick, *Transparency is the New Privacy: Blockchain's Challenge for the Fourth Amendment*, 23 Stan. Tech. L. Rev. 114, 117 (2020). A blockchain is a digital, public ledger to which participants can add information about their transactions, instead of funneling that information to a central repository. That does not mean, however, that participants can write on the ledger to say whatever they please; rather, the responsibility for "validat[ing]" the transaction is "distributed," *i.e.*, "many computers … in a network" (known as "nodes") "share and store the same data at the same time" and "review[] the … ledger[]" to verify the validity of each transaction. *See* Belonick, *supra*, at 128-130. This distributed validation maintains the integrity of the information, much in the way that a central authority—like a bank—would otherwise serve as a clearinghouse of accurate information. *See id*. Blockchain removes the role of the central authority, and instead supplants it with a democratized, decentralized approach. *Id.*

To add data to the blockchain, users typically use a "wallet," which is, in simple terms, software that provides a means of interfacing with the blockchain. *See How Does Blockchain Work?*, Stanford Online (last visited Sept. 27, 2023), https://online.stanford.edu/how-does-blockchain-work. The wallet generates two keys, a private key and a public key, which are "created and linked [together] by a mathematical algorithm"—this creates a system in which "the public key scrambles data" that "only the [associated] private key can unscramble." *See* Belonick, *supra*, at 126-127. The public key is viewable on the blockchain, "can be shared with others with whom one wishes to interact," and is used to send information (not unlike an account number or email address). *See id*. The private key, by contrast, is "known only to an individual user" and is used to access information (not unlike a password). *See id*. If one user wants to send data to another, he or she will use the intended recipient's public key to "scramble" or "encrypt" the data and send it over the blockchain. *See id*. Only the recipient's private key, which remains unknown to all but its holder, can unscramble this data. *See id*. (And if a private key is lost, it is lost forever, and the contents of the "wallet" cannot be retrieved.) Through this system, users "can … share data privately over public networks, fully assured that no one else can interfere, even if the world can see scrambled data passing." *See id*.

A. In the typical blockchain transaction, critical details about a transaction, including a user's identity, remain private even though certain details about the transaction are widely publicized.

Although a blockchain is effectively a public ledger, blockchain entries do not reveal everything there is to know about a particular transaction. *See Belonick*, *supra*, at 134-136. Those reviewing publicly available blockchain data may be able to see the date, time, and amount of a particular crypto transaction, along with the public key addresses involved. But the identifying details of the transaction's participants are pseudonymized—that is, the blockchain "ledger" does not reveal the real-world identities associated with the public addresses. *See id.* at 134. Thus, while blockchain is open in that "[t]he public can see that someone is sending an amount to someone else," it also provides users with a measure of privacy by omitting "information linking the transaction to anyone." *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 6, https://bitcoin.org/bitcoin.pdf. In other words, even with blockchain's openness, users can expect privacy since their crypto transactions will not be tied to their real-world identities.

Some courts have operated on a technical misunderstanding of how blockchain technology works. The Fifth Circuit in *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020), for example, noted that "it is possible to discover the owner of [an] address by analyzing the blockchain." *See id*. at 309. That is not true (or, at the very least, the "possibility" is largely theoretical). Generally, "[b]lockchain

user[s] can … expect not to be identified" based solely on that information which is publicly viewable on the blockchain. *See* Belonick, *supra*, at 135. While it *might* be possible to "connect[] an anonymous address's pattern of activity … to specific IP addresses, and thus to real-world users," doing so requires "specialized and intensive" methods that are "currently the realm only of experts." *See id*. at 135, 160. And even where experts engage in such "specialized and intensive methods"—requiring time-consuming data collection and "complex probability analyses"—in many cases it will not be possible to discern the identity of a wallet's owner. *See id.* at 134-135, 160.

B. Crypto transactions can take place either on the blockchain itself or via third-party crypto exchanges, which are required to collect information concerning their customers.

While crypto users often transact directly with one another on the blockchain, users may also trade in crypto assets through "exchanges."[3] These exchanges are,

[3] By "exchange," we refer to centralized exchanges where the exchange serves as an intermediary.

There are two types of exchanges: centralized exchanges and de-centralized exchanges. Centralized exchanges "typically require that users place assets in their custody before trading." Benedict George & Toby Bochan, *Centralized Exchange (CEX) vs. Decentralized Exchange (DEX): What's the Difference?*, CoinDesk (Nov. 15, 2022, 11:12 AM), https://www.coindesk.com/learn/centralized-exchange-cex-vs-decentralized-exchange-dex-whats-the-difference/. Decentralized exchanges, by contrast, require users to maintain their own wallets to "hold their own assets." *Id.* While both allow users to find a market for their crypto assets, decentralized exchanges do not "act[] as a financial intermediary or counterparty" and instead facilitate peer-to-peer transactions. *Id.*

in essence, "businesses that … facilitate third-party transactions of traditional currency for cryptocurrency" (or, in some cases, one type of cryptocurrency for another). *See Zietzke v. United States*, 426 F. Supp. 3d 758, 762 (W.D. Wash. 2019). A user may use an exchange for a number of reasons. An exchange may provide the easiest way of participating in a crypto network—*i.e.*, by providing a ready marketplace to trade fiat money (such as U.S. dollars) for crypto assets. In addition, exchanges can be perceived to "offer an extra layer of security and reliability when it comes to transactions and trading." *See Cryptocurrency Exchanges*, CFI (last visited Oct. 16, 2023), https://corporatefinanceinstitute.com/resources/cryptocurrency/cryptocurrency-exchanges/. They do so through services such as a "hosted wallet service," *Zietzke*, 426 F. Supp. at 762, which is wallet software maintained by the exchange as opposed to the user. *See Hosted Wallet*, CipherTrace (last visited Sept. 27, 2023), https://ciphertrace.com/glossary/wallet-hosted/. These hosted wallets, unlike the typical wallet, generally "provide[] … users with the possibility to restore lost credentials, perform[] backups and guarantee[] security of the user's funds." *See Hosted Wallet Explained*, Freewallet (May 30, 2018), https://freewallet.org/blog/hosted-wallet-explained/#What%20Is%20A%20Hosted%20Wallet?. (Contrast that to a "self-hosted" wallet on the blockchain itself, with public and private keys—the latter of which is irrecoverable once lost.)

Adding the middleman of an exchange has certain benefits, but it also imposes additional burdens and obligations on a user. The U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") considers exchanges to be "money services businesses,"[4] which are required under the Bank Secrecy Act, 31 U.S.C. § 5311, to, among other things, obtain due diligence about customers ("know your customer" or "KYC") and implement anti-money laundering programs. That means, in order to participate in crypto transactions through an exchange, users must provide information about their identities to participate in such transactions. Moreover, unlike those who transact directly on the blockchain, those who use an exchange generally do not have their own private keys. Rather, the use of a hosted wallet service typically means that the exchange "receive[s], store[s], and transmit[s] cryptocurrency transactions on behalf of their accountholders" and that the "accountholder generally does not have access to the cryptographic keys themselves." *See* Office of the Comptroller of the Currency, *Interpretive Letter #1172*, at 1 n.3 (Oct. 2020), https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf.

[4] FinCEN, *Guidance FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* 2 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

C. Regardless of whether one transacts directly on the blockchain or through an exchange, knowing the identity of a wallet's owner can reveal sensitive and nonpublic information about the user.

Because crypto transactions are automatically—and permanently—logged on "[b]lockchain's lengthy and permanent ledger records" for all to see, knowing the identity of a wallet's owner can reveal years of sensitive and nonpublic information about the owner's day to day affairs. *See* Belonick, *supra*, at 152-153. As noted *supra* pp. 7-8, a blockchain is unique—it is "public" in the sense that everyone can see a transaction, but it is "private" in the sense that certain details are kept out of public view. With knowledge of the wallet-owner's identity, those private details would instantly become public, made transparent through a simple review of the blockchain's public ledger. The resulting intrusion would be more far reaching, and more severe, than, for example, a bank revealing specific information about a customer account. In that case, there are built in limitations on the intrusion—*i.e.*, the intrusion is limited to one's transaction history at a particular bank during a specific period, and does not provide the Government with a broader window into information not contained within the records obtained. By contrast, knowledge of the real-world identity behind a public key or account number (in the case of an exchange) would allow an observer to easily tie years of crypto transactions to a particular individual and, in the process, reveal otherwise unknowable "patterns in their social contacts and affiliations." *See id.*

For example, knowing a user's identity would allow one to easily track years of the user's consumption and spending habits—what they buy, who they buy from, and how often—especially as cryptocurrencies become more prominent in retail transactions and in making payroll. *See, e.g.*, Robin Singh, *Getting Paid in Cryptocurrency? Learn the Tax Laws*, Forbes (July 9, 2021, 7:20 AM), https://www.forbes.com/sites/forbesfinancecouncil/2021/07/09/getting-paid-in-cryptocurrency-learn-the-tax-laws/?sh=4137b7fb579e; *Who Accepts Bitcoin in 2023?*, Cryptonews (last visited Oct. 16, 2023), https://cryptonews.com/guides/who-accepts-bitcoin.htm. Moreover, knowing the identity of a wallet's owner (or an account holder) may allow one to ascertain that a user has, through donations of cryptocurrencies, supported particular social movements or causes—information that could be revealed to those who oppose such causes. For example, one who donates to Ukraine relief efforts via cryptocurrencies could have their identity and the fact of their donation disclosed to Russia. *E.g.*, MacKenzie Sigalos, *Ukraine Has Raised More Than $54 Million as Bitcoin Donations Pour In to Support the War Against Russia*, CNBC (Mar. 3, 2022, 5:39 PM), https://www.cnbc.com/2022/03/03/ukraine-raises-54-million-as-bitcoin-donations-surge-amid-russian-war.html. And knowing the identity of a wallet's owner (or an account holder) might allow prying eyes to peek at private and intimate transactions—such as purchases of certain medications (like Viagra) or payments for medical procedures (such as an

abortion)—that people understandably would like to keep private. *See Cryptocurrencies And Medical Bills: The New Way To Pay For Healthcare?*, Healthcare Business Today (Nov. 4, 2022), https://www.healthcarebusinesstoday.com/cryptocurrencies-and-medical-bills-the-new-way-to-pay-for-healthcare/.

Aside from financial information, as the use cases for crypto and blockchain technology continue to grow, knowledge of a user's real-world identity could result in the exposure of other types of sensitive and nonpublic information. For example, blockchain technology is being used to track patient medical histories, such that revealing the identity behind a patient's pseudonymous public key could result in the unintended disclosure of the patient's private medical information to a third party. *See* Steve Alder, *The Benefits of Using Blockchain for Medical Records*, HIPAA Journal (Sept. 26, 2017), https://www.hipaajournal.com/blockchain-medical-records/. Blockchain is even being used by some state governments to "secure government documents," meaning that access to a user's real-world identity could reveal "sensitive data and agency information." *See* Sam Daley, *33 Blockchain Applications and Real-World Use Cases*, BuiltIn (Mar. 2, 2023), https://builtin.com/blockchain/blockchain-applications; Anastasiya Haritonova, *Blockchain in Government: Use Cases, Challenges, and Real-Life Projects*, Pixelplex (Dec. 11, 2022), https://pixelplex.io/blog/blockchain-in-government-processes/. And blockchain technology is also being used in a host of

other areas, such as social media (and traditional media), supply chain management, and "smart" contracting, *see* Daley, *supra*; each such use presents the potential for exposure of unique types of private and personal information should a user's real-world identity be revealed.

II. There is a reasonable expectation of privacy in crypto transactions—even ones conducted through an exchange.

"[A] foundational pillar" of crypto and blockchain technology is privacy: that "decentralized data systems" will allow users to wrest control of their information from centralized repositories of information, such as Facebook and YouTube. David Z. Morris, *The Privacy Boom is Going to Change Everything*, CoinDesk (Jan. 24, 2022, 12:14 PM), https://www.coindesk.com/layer2/2022/01/24/the-privacy-boom-is-going-to-change-everything/. Bitcoin, for example, reflects a mission of digital privacy to "create digital money that would be as anonymous as physical cash," and it achieved that mission in part by being "sent electronically without needing to pass through a central authority like a bank." Nathaniel Popper, *Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin*, N.Y. Times (May 15, 2015), https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html.

In other words, privacy is a foundational pillar of blockchain technology—and it serves as one of the main reasons why an individual user might lean on such technology in the first place. The decentralized nature of blockchain allows users to

claw back some of the information that they surrender to a central authority, such as a bank or a tech company, and to keep that information from public view.

So, it was wrong for the district court to conclude that there is no reasonable expectation of privacy in crypto transactions—even those that take place on crypto exchanges. JA083 – JA086. That conclusion was incorrect for two reasons. First, the court failed to recognize that blockchain users expect certain details of their transactions to remain unknown and thus private, even when users transact via an exchange. Second, the court failed to account for the sweeping nature of the summons here—one that seeks to aimlessly dig a mile wide and a mile deep in searching for potentially useful information.

A. There is a societal expectation that crypto and blockchain can be used to ensure privacy, even when a third-party exchange is involved.

Contrary to the district court's conclusion, crypto users possess a reasonable expectation of privacy in their personal identifying information held by third-party exchanges. "Whether the Fourth Amendment[] … has been violated depends on whether the person asserting a … violation had a reasonable expectation of privacy in the place searched or the thing seized." *United States v. Thornley*, 707 F.2d 622, 624 (1st Cir. 1983). This analysis is ultimately driven by what "society is prepared to recognize as 'reasonable.'" *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (citation omitted). In the past, the Supreme Court has suggested that "a person has no

legitimate expectation of privacy in information he voluntarily turns over to third parties," for such an individual "'takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.'" *See Smith*, 442 U.S. at 743-744 (citation omitted). But, on the other hand, the Court has recently clarified that the "third-party doctrine" may "not by itself overcome the user's claim to Fourth Amendment protection," if the "nature" of the records at issue are sufficiently "unique." *See Carpenter*, 138 S. Ct. at 2216-2217.

Here, crypto users reasonably expect that their crypto assets can be used in a way that maintains privacy—an expectation that is not lost even if users transact through a third-party exchange, given the unique nature of the records involved. First, as a general matter, there is a strong societal expectation that crypto can be used in a way that maintains privacy. Privacy, after all, is a central pillar of crypto and is an inherent feature of blockchain. *See* Belonick, *supra*, at 126. Privacy is why "[b]lockchain users are usually represented by … cryptographic addresses" and why "the real-world identities" of blockchain users are typically "kept entirely private." *See* Belonick, *supra*, at 134. True, other information is published on the blockchain for all to see. *See supra* p. 7. But that some information is publicly viewable does not "frustrate[]" the "expectation of privacy" in other information that is not—particularly, a user's identity. *See United States v. Jacobsen*, 466 U.S. 109, 117 (1984) ("Fourth Amendment is implicated … if the authorities use information

with respect to which the expectation of privacy has not … been frustrated"); *see also Katz v. United States*, 389 U.S. 347, 351 (1967) ("what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected"). As discussed, *see supra* pp. 7-8, such information remains unknowable "absent highly intricate efforts by an unusually sophisticated" actor. *See* Belonick, *supra*, at 135. The result is that "sophisticated blockchain user[s] can reasonably expect not to be identified." *See id*.

Second, and importantly, crypto users reasonably expect this same level of privacy, even if they transact through a third-party exchange, due to the unique and sensitive nature of the records involved. The Supreme Court confirmed in *Carpenter* that one's expectation of privacy in information does not disappear merely because that information has been provided to a third party for the third party's business records. *See* 138 S. Ct. at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere."). In *Carpenter*, the Court addressed whether the defendant possessed a reasonable expectation of privacy in cell site location information ("CSLI")—data that revealed the defendant's historical movements—maintained by "third party" wireless carriers. *See id*. at 2212-2213. The Court answered that question in the affirmative, holding that the relevant Fourth Amendment analysis is not based "solely on the act of sharing" the information with a third party, but on "the nature of the particular documents sought." *See id*. at 2219

(citation omitted). Because the "nature" of the CSLI at issue was "unique," "qualitatively different," and "an entirely different species of business record"—in that it provided a "retrospective" and "detailed chronicle of a person's" movements and "associations" that was "otherwise unknowable"—the Court concluded that it was deserving of Fourth Amendment protection. *See id*. at 2216-2220.

Like the CSLI in *Carpenter*, the combination of a crypto exchange's know-your-customer records and transaction data is an "entirely different species of business record" deserving of Fourth Amendment protection. *See id.* at 2222. Here, like in *Carpenter*, there is a "retrospective quality" to the information, in that knowing the identity of a wallet's (or account's) owner can reveal years of sensitive and nonpublic information about the owner's day to day affairs. *See id.* at 2218; *see also* Belonick, *supra*, at 158-159 ("[A] search of an immutable blockchain could instantly reveal years of activities … as blockchain … scrupulously and permanently record[s] when, where, and what we are doing"). The Government would thus obtain a "detailed chronicle of a person's" blockchain movements and "associations"—precisely like that which the *Carpenter* Court sought to prevent. *See* 138 S. Ct. at 2217-2220.

Moreover, the personally identifying information at issue here, like the CSLI in *Carpenter*, would be "otherwise unknowable" to law enforcement, or even anyone other than the exchange, absent a broad, intrusive inquiry like the John Doe

summons issued here. Courts have operated under the misimpression that one can simply "analyze the … blockchain" to discern the identity of a party. *Gratkowski*, 964 F.3d at 309. Not true. If such identification were easily possible through publicly available information, that would knock over one of the central pillars of crypto: the ability to keep transactions private, away from prying eyes. At the outset, a public key holder's identity cannot be discerned through ordinary means; that identity *might* be discernible only by using powerful, sophisticated tools beyond the general public's reach. *See Carpenter*, 138 S. Ct. at 2218 (existence of a search must "take account of more sophisticated systems that are already in use or in development") (citation omitted); *see also* Belonick, *supra*, at 145 ("De-anonymization is currently the purview of experts willing to spend months on data gathering and analysis"). A John Doe summons, as used in the context here, seeks information—a user's identity and transaction history—that would otherwise remain unknowable absent resort to "sophisticated systems" and extraordinary means that are "not in general public use." *See Kyllo v. United States*, 533 U.S. 27, 34-36 (2001).

B. In crypto cases, John Doe summonses have been used as dragnets.

The IRS may issue a so-called "John Doe summons" to "ascertain[] the correctness of any return, mak[e] a return where none has been made, determin[e] the liability for any person for any internal revenue tax or the liability at law or in

equity of any transferee … or collect[] any such liability." 26 U.S.C. § 7602(a). The statute allows, in pertinent part, the IRS to issue a summons "[t]o examine any books, papers, records, or other data which may be relevant or material to such inquiry." *Id.*

To obtain a John Doe summons, the IRS must establish, in a court proceeding, that:

> (1) the summons relates to the investigation of a particular person or ascertainable group or class of persons,
>
> (2) there is a reasonable basis for believing that such person or group or class of persons may fail or may have failed to comply with any provision of any internal revenue law, and
>
> (3) the information sought to be obtained from the examination of the records or testimony (and the identity of the person or persons with respect to whose liability the summons is issued) is not readily available from other sources.

26 U.S.C. § 7609(f); *Harper v. Rettig*, 46 F.4th 1, 3-4 (1st Cir. 2022).

In the crypto context, the IRS has tried to use John Doe summonses to obtain wide swaths of information about a large number of users from crypto exchanges—users who were not previously suspected of any wrongdoing. Exchanges and courts, however, have pushed back, to some extent. When the IRS issued a John Doe summons to Coinbase, seeking "nine categories of 'information regarding United States persons'" who "conducted transactions in a convertible virtual currency" over a two-year period, Coinbase objected, so the IRS narrowed the summons to collect

less information from a smaller group of users—those accounts with more than $20,000 "in any one transaction type." *Harper*, 46 F.4th at 3-4 (quoting *United States v. Coinbase, Inc.*, No. 17-cv-01431-JSC, 2017 WL 5890052, at *1-2 (N.D. Cal. Nov. 28, 2017)). The district court still declined to enforce the subpoena in its entirety, noting the fact that the $20,000 threshold meant "the Government is seeking records on over 10,000 account holders." *Coinbase*, 2017 WL 5890052, at *6. The *Coinbase* court further narrowed the scope of the summons by tossing out the Government's demand for "[r]ecords of Know-Your-Customer diligence" and records regarding third-party access to Coinbase accounts and wallets. *Id.*

Several years after *Coinbase*, the IRS issued a John Doe summons to Kraken, seeking five years' worth of extensive information regarding nearly 60,000 users who engaged in at least $20,000 of transactions on Kraken's exchange. *United States v. Payward Ventures, Inc.*, No. 23-mc-80029-JCS, 2023 WL 4303653, at *7-8 (N.D. Cal. June 30, 2023). The information sought included not just "basic registration, identification, and transaction information," but also "complete user preferences, any other records of Know-Your-Customer due diligence, and all correspondence between Kraken and [a user] or any third party with access to the account pertaining to the account." *Id.* at *7 (internal quotations omitted). Kraken objected on the grounds that the IRS sought "unfettered access to the private financial and personal information of thousands of otherwise law-abiding users that

the IRS has no interest in auditing." *Id.* at *18. The court concluded that many of the IRS's requests were overbroad, and limited the IRS's collection of information to certain basic identifying information, and discrete batches of transactional information. *Id.* at *29.

When a third party challenges a John Doe summons, it may usually do so only on overbreadth or burden grounds; as the existence of this case suggests, exchanges likely do not have standing to raise Fourth Amendment concerns about how providing information might intrude into a particular user's privacy. *Cf. Tiffany Fine Arts, Inc. v. United States*, 469 U.S. 310, 320 (1985) (noting Congress's concern in enacting the John Doe summons statute that "the party receiving a summons would not have a sufficient interest in protecting the privacy of the records if that party was not itself a target of the summons"). Accordingly, the fact that exchanges have been required to provide the IRS with basic identifying information about a user's account information does not mean that there is no reasonable expectation of privacy in that information, or that there are not serious Fourth Amendment concerns about how the IRS has gone about collecting even the limited information that courts have grudgingly authorized the agency to collect.

The IRS's attempts to collect information a mile wide (*i.e.*, on a large number of individuals) and a mile deep (*i.e.*, identifying information and the transactions associated with an individual), is alarming. As the Supreme Court observed nearly

a century ago, "[a]nyone who respects the spirit as well as the letter of the Fourth Amendment would be loath to believe that Congress intended to authorize one of its subordinate agencies to sweep all our traditions into the fire, and to direct fishing expeditions into private papers on the possibility that they may disclose evidence of crime." *FTC v. Am. Tobacco Co.*, 264 U.S. 298, 305-306 (1924) (citation omitted). The John Doe summons statute is no different: "Congress determined that when the IRS uses its summons power not to conduct a legitimate investigation of an ascertainable target, but instead to look around for targets to investigate, the privacy rights of taxpayers are infringed justifiably." *Tiffany Fine Arts*, 469 U.S. at 320; *see also* H.R. Rep. No. 94-658, at 311 (1975) ("[T]he committee does not intend that the John Doe summons is to be available for purposes of enabling the Service to engage in a possible 'fishing expedition.'"). The privacy concerns are only diminished if the summons "seeks information relevant to a legitimate investigation of a particular taxpayer." *Tiffany Fine Arts*, 469 U.S. at 321.

Accordingly, when the IRS uses John Doe summonses "to look around for targets to investigate," *id.* at 320, the expectations of privacy—and the nature of the Fourth Amendment intrusion—are different than when the IRS uses a John Doe summons to seek out information about a specific taxpayer whose name and taxpayer ID may not be known, but other facts may reveal the individual's identity. *Cf. Byers v. IRS*, 963 F.3d 548, 555-56 (6th Cir. 2020) (noting the IRS may be able

to fish "in the context of a summons *targeting a named taxpayer*" (quoting *United States v. Giordano*, 419 F.2d 564, 568 (8th Cir. 1969)) (emphasis added)).

C. The district court's reliance on *Miller* was misplaced, as the IRS's inquiry here is far more intrusive than the request for bank records in *Miller*.

The district court made two mistakes in holding that Harper has no Fourth Amendment claim here. Both mistakes arose from the district court's incorrect application of the third-party doctrine, which relied on the overly simplistic understanding that, once information is surrendered to a third party, like "bank records and customer information held by financial institutions," any expectation of privacy evaporates. JA082. In making that observation, the district court cited *United States v. Miller*, 425 U.S. 435, 444 (1976), where the Supreme Court held that a bank depositor had "no Fourth Amendment interests" in a bank's record of his accounts and transactions.

Most critically, the court overlooked the nature of the Government's investigation here, which affects relative expectations of privacy. *Miller* involved a bank subpoena that already established the identity of the person for whom information was sought. *See* 425 U.S. at 437-438. Similarly, *Gratkowski* addressed a grand jury subpoena seeking information on only those users who had transacted with particular "addresses" that the Government had already established were tied to a website promoting criminal activity. *See* 964 F.3d at 309. In other words,

neither case involved a fishing expedition, but instead concerned targeted inquiries of a specific individual or accounts. By contrast, the John Doe summons in Harper's case sought a broad swath of information regarding more than 10,000 users. That is akin to the Government going to the bank in *Miller* and asking the bank to dump out every single deposit and withdrawal slip, wire transfer record, and every other piece of paper that the bank might have on *all* of its account holders (or perhaps the account holders at a particular branch), all because the Government thinks it might find some proof of actionable activity in that pile of papers. This is the sort of indiscriminate and unparticularized fishing expedition that the Fourth Amendment aggressively guards against. *Am. Tobacco*, 264 U.S. at 305-306.

The court also failed to recognize the privacy interest that is not only inherent to crypto, but essential to it. Bank accounts are centralized; crypto transactions are not. An exchange may provide some centralized functions, but that does not mean an individual expects that crypto will no longer be crypto, *i.e.*, shielded from the prying eyes of the public. The contrast between the centralization of a bank, and the decentralization of crypto, is important. *Miller* held that that the defendant lacked a reasonable expectation of privacy in copies of his checks, deposit slips, and bank statements, primarily because information regarding a person's bank transactions is generally not considered private. *See* 425 U.S. at 442. Instead, such records, the Supreme Court observed, are merely "negotiable instruments … used in commercial

transactions" between counterparties, and "contain only information voluntarily conveyed to the banks and … their employees in the ordinary course of business"; in other words, counterparties and intermediaries are all aware of who is sending, and who is receiving, in a particular transaction. *See id.*

But the same is not true of crypto transactions. Blockchain, by design, is decentralized, and thus dispenses with the need for an intermediary altogether—let alone the need to "convey[]" anything to one. *See supra* pp. 5-6. Blockchain is also designed to allow parties to transact using pseudonymous keys and account numbers; thus, unlike in bank transactions, counterparties to a crypto transaction may not know the real-world identities of those with whom they are transacting. *See supra* pp. 7-8. In short, by eliminating inquiring intermediary eyes and allowing users greater control over disclosure of their real-world identities, the expectation of privacy users have with respect to their crypto transactions is reasonably higher than that which they can expect in their traditional bank transactions.

And this remains true even when an exchange is involved on one side of the transaction. For one, an exchange's presence does not mean that all the details of a particular transaction are revealed to a third party. While the exchange may know the identity of one transacting party, other details of the transaction—like who is on the other side—will remain private. *See supra* pp. 5-6. Along these same lines, the involvement of an exchange does not change that counterparties to a transaction can

remain pseudonymous as to each other. That is, counterparties may not know each other's identities, even if that information is known by the exchange as to one of the participants. *See supra* pp. 5-6. Finally, the information held by a crypto exchange is unlike the bank records addressed in *Miller*, which are designed to be, and in fact, are "exposed to [bank] employees in the ordinary course of business." *See* 425 U.S. at 442. By contrast, the identity of the person responsible for an exchange account is not exposed to the vast majority of the exchange's employees—indeed, "[e]mployee access is heavily restricted." *See How Does Coinbase Use My ID?*, Coinbase (last visited Sept. 27, 2023), https://help.coinbase.com/en/coinbase/privacy-and-security/other/how-does-coinbase-use-my-id.

* * * * *

Not all John Doe summonses will raise constitutional problems like the summons here. But the summons directed at Coinbase, which Harper now contests (as it relates to him), plainly raises the type of Fourth Amendment problem that Congress sought to prevent through procedural guardrails: an ambitious fishing expedition, one that searches for taxpayers to target, rather than to collect information on an already existing target. The summons statute was not intended to allow the IRS to inquire of a third party the identity of every person who may owe

taxes. Doing so intrudes on the privacy interests of individuals like Harper, in a manner that violates the Fourth Amendment.

CONCLUSION

This Court should reverse the district court's decision on Harper's Fourth Amendment claim.

Respectfully submitted,

/s/ Andrew Kim
Andrew Kim
Gabe Maldoff
GOODWIN PROCTER LLP
1900 N Street, N.W.
Washington, D.C. 20036-1612
Tel.: (202) 346-4000
andrewkim@goodwinlaw.com

Counsel for Amicus Curiae
Paradigm Operations LP

Rodrigo Seira
PARADIGM OPERATIONS LP
548 Market Street
San Francisco, CA 94104
Tel.: (415) 986-9283

Omer Tene
Christopher J.C. Herbert
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, MA 02210
Tel.: (617) 570-1000

Date: October 20, 2023

CERTIFICATE OF COMPLIANCE

I hereby certify that this document complies with the type-volume limitations of Federal Rules of Appellate Procedure 29(a)(5) and 32(a)(7)(B) because it contains 6,437 words, excluding the parts of the document exempted by Rule 32(f).

This document complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced, 14-point Times New Roman font, using Microsoft Word.

Dated: October 20, 2023

/s/ Andrew Kim

Andrew Kim
GOODWIN PROCTER LLP
1900 N Street, N.W.
Washington, D.C. 20036-1612
Tel.: (202) 346-4000
andrewkim@goodwinlaw.com

Counsel for Amicus Curiae
Paradigm Operations LP

CERTIFICATE OF SERVICE

I hereby certify that I filed the foregoing brief with the Clerk of the United States Court of Appeals for the First Circuit via the CM/ECF system on this 20th day of October 2023. I certify that service will be accomplished through the CM/ECF system upon the registered participants listed below, and that service by U.S. Mail was executed on non-registered participants.

Sheng Tao Li
shenghiskhan@gmail.com
Richard Abbott Samp
rich.samp@ncla.legal
New Civil Liberties Alliance
1225 19th Street, N.W.
Suite 450
Washington, DC 20036

Counsel for Plaintiff-Appellant

Seth R. Aframe
seth.aframe@usdoj.gov
United States Attorney's Office
53 Pleasant Street, 4th Floor
Concord, NH 03301

Kathleen E. Lyon
Kathleen.E.Lyon@usdoj.gov
Edward J. Murphy
Edward.J.Murphy@usdoj.gov
U.S. Department of Justice, Tax Division
P.O. Box 502
Ben Franklin Station
Washington, DC 20044

Counsel for Defendants-Appellees

/s/ Andrew Kim

Andrew Kim
GOODWIN PROCTER LLP
1900 N Street, N.W.
Washington, D.C. 20036-1612
Tel.: (202) 346-4000
andrewkim@goodwinlaw.com

Counsel for Amicus Curiae
Paradigm Operations LP