No. 24-336

IN THE

Supreme Court of the United States

BINANCE, ET AL.,
Petitioners,

v.

JD ANDERSON, ET AL.,
Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Second Circuit

BRIEF OF THE CRYPTO COUNCIL FOR INNOVATION AS *AMICUS CURIAE* IN SUPPORT OF PETITION FOR CERTIORARI

Jason P. Gottlieb
Counsel of Record
Daniel C. Isaacs
Michael Mix
Rachel Fleder
Vani Upadhyaya
MORRISON COHEN LLP
909 Third Avenue
New York, New York 10022
(212) 735-8600
jgottlieb@morrisoncohen.com

Counsel for Amicus Curiae

October 25, 2024

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

STATUTES AND RULES

OTHER AUTHORITIES

Lyllah Ledesma, *A $1.4T Financial Giant Expands Its Money Market Fund on Polygon*, CoinDesk (Apr. 26, 2023), https://www.coindesk.com/business/2023/04/26/a-14t-financial-giant-expands-its-money-market-fund-on-polygon 14

Darob Malek-Madani, *How the Internet Works*, National Real Estate Advisors (Jan. 2021), https://natadvisors.com/wp-content/uploads/2019/08/How-The-Internet-Works-Whitepaper-Final.pdf 5, 6

Angelica Mari, *Brazil Develops Blockchain Network to Support ID Rollout*, Forbes (Sept. 28, 2023), https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-develops-blockchain-network-to-support-id-rollout/..... 18

Dillin Massand, *Dubai: Launching a Crypto Regulatory Arm to Become a Global Financial Power*, CoinDesk (June 27, 2023), https://www.coindesk.com/consensus-magazine/2023/06/27/dubai-launching-a-crypto-regulatory-arm-to-become-a-global-financial-power/ 17

Dora Mekouar, *Here's Where the Internet Actually Lives*, VOA (Feb. 17, 2020), https://www.voanews.com/a/usa_all-about-america_heres-where-internet-actually-lives/6184090.html/..... 8

INTEREST OF *AMICUS CURIAE* [1]

The Crypto Council for Innovation ("CCI") is the premier global alliance of industry leaders with a mission to communicate the opportunities presented by blockchain technology and digital assets and demonstrate their transformational potential. Indeed, blockchain technology serves as the infrastructure for a new generation of the internet. CCI's members, which include leading global companies and investors in the industry, share the goal of encouraging responsible global regulation of blockchain technology to unlock economic potential, improve lives, foster financial inclusion, protect national security, and combat illicit activity. CCI believes that achieving these goals requires informed, evidence-based policy decisions realized through collaborative engagement with regulators and industry.

CCI's particular interest in this case arises because the Second Circuit held, in part, that components of internet infrastructure—specifically, servers on which transactions "matched"—were located in the United States, factoring into making those transactions "domestic" for purposes of

---

[1] No counsel for either party authored this brief in whole or in part, nor did any party or other person or entity other than *amicus curiae*, its members, or its counsel make a monetary contribution to the brief's preparation or submission. Counsel of record for all parties received notice at least ten days prior to the due date of the intention of *amicus curiae* to file this brief.

determining territoriality. Pet'r's App. 12a. CCI respectfully disagrees with that notion, for legal, technological, and policy reasons. Were that Second Circuit holding to stand, the doctrine set forth in *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247 (2010) would be eviscerated, leading to devastating consequences for the blockchain industry, an array of other American businesses, and foundational principles of comity.

SUMMARY OF ARGUMENT

The Second Circuit improperly considered the geographical location of internet infrastructure in its decision that certain transactions were not sufficiently "extraterritorial" to be outside the scope of the relevant federal statutes. In particular, the Second Circuit held that internet transactions allegedly passed through servers in California, and that digital data was allegedly stored on servers in California. Pet'r's App. 15a. As a result, the Second Circuit held that the extraterritoriality doctrine voiced in *Morrison* was inapplicable. In doing so, the Second Circuit erred.

For the internet to work, most of it has to be invisible. When a user sends an email, or buys a book from an online bookstore, or comments on a news article, data signals sent by the user pass through an array of internet infrastructure—local servers, intermediary servers, remote servers, internet service providers, routers, data centers, and the many other pieces of internet architecture required to make it all work. Thanks to the miracles

of modern engineering, those pieces of physical infrastructure can be located anywhere. A user in Washington, D.C. can place an online order for a book from a Parisian bookstore, and that "buy" signal may be routed through internet providers in Virginia, Pennsylvania, and New Jersey, servers in California, relayers in Canada, Iceland, and the U.K., to the bookstore in France, who "settles" that transaction on a server in Germany and on the servers of a book-shipper in Ireland, before routing confirmation signals back in the same way (or a different way)—all within a few hundred milliseconds.

Most users, most of the time, care about none of that. Nor should they. Users have little choice what internet infrastructure is used, or where. And a world where users had to care about each of those steps—and consider whether they were subjecting themselves to the law of each of those states or nations—would bring the world of internet commerce to a screeching halt.

One exciting new technology revolutionizing internet infrastructure is blockchain technology, which has seen a meteoric rise in usage in the last decade due to its increased cybersecurity, efficiency, and resilience. But that technology relies on an even more complex tangle of its own infrastructural geography. A blockchain functions by recording every transaction on that blockchain on every "node" in the chain, which is the source of its increased resilience—if one node fails, all other nodes provide redundancy, and the chain's records are unaffected.

A blockchain is analogous to a global public computer and database, operated and maintained by all of the nodes. But those nodes, and the "validators" who verify transactions on the blockchain, can be located anywhere in the world. The Ethereum blockchain (one of the largest) has over 6,300 nodes all over the world, meaning that any Ethereum blockchain transaction will "settle" on servers in the U.S., Germany, Canada, the U.K., France, South Korea, Singapore, the Netherlands, Australia, and many other countries.

Users do not need to care about that geographical quirk either—as far as users are concerned, it is all "back-office" internet infrastructure. If the "location" of a blockchain transaction triggered the applicability of law and jurisdiction of any and all countries where blockchain transactions settle, then every user could be affected by the laws of dozens of countries, and even different states within those countries, for every transaction.

The Second Circuit erred in considering back-office internet infrastructure, such as the location of Amazon Web Services ("AWS") servers, as a factor to judge whether the extraterritoriality doctrine should apply. That result, if sustained, would seriously impair American internet infrastructure business, causing it to move offshore (with many attendant disadvantages for Americans and U.S. law enforcement). It would also corrode the doctrine of comity, placing Americans at risk of being sued in foreign countries for using internet infrastructure that touches foreign nations. It further would risk

foreigners suing foreign companies in U.S. courts, causing judicial overload. Given the global primacy of American internet infrastructure, it is rare that internet transactions do not touch internet infrastructure in the U.S. at some point. If that fact potentially subjected transactions anywhere in the world to litigation in the U.S., the result would moot *Morrison*, devastate the blockchain industry, negatively affect a host of other federal laws beyond blockchains and digital assets, and cast shadows over the doctrine of comity. The Second Circuit decision directly challenges this Court's extraterritoriality holdings, and this Court should grant certiorari in this clean vehicle to reverse the Second Circuit's decision.

STATEMENT OF FACTS

I. HOW INTERNET TRANSACTIONS WORK

Internet transactions transmit data through a complex array of internet infrastructure. When a user initiates an internet transaction, the user's request emanates from that user's device, and is broken down into smaller data packets that travel through the user's Internet Service Provider ("ISP") network.[2] The data packets then travel through the

---

[2] *See* Darob Malek-Madani, *How the Internet Works*, National Real Estate Advisors (Jan. 2021), at 4, https://natadvisors.com/wp-content/uploads/2019/08/How-The-Internet-Works-Whitepaper-Final.pdf. ISPs are "networks which provide users access to the broader internet." *Id.* They are "typically owned and operated by … large telecom companies," such as Verizon or Comcast. *Id.*

internet backbone—the core infrastructure of the internet, consisting of a global system of interconnected networks.[3] The data will eventually reach its destination server, which will process the request and send back its response to the user's device.[4] Both ways, the data travels through a complex network of several routers, servers, and switches located in various data centers, and may pass through firewall appliances and proxy gateways, among other applications, many of which can be geographically dispersed.

This underlying infrastructure is essentially invisible to users who send emails, access websites, and complete online purchases without any consideration of the many components involved.

The invisibility of the internet's complex infrastructure is integral to its success. Users can focus on the content of whatever web page or application they are using without being distracted by the complex network of cables, routers, servers,

---

[3] *See* Rus Shuler, *How Does the Internet Work*, Pomeroy IT Solutions (2002), https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm. A router is a networking device, "operat[ing] as a switch at the intersections of networks," that directs packets of data between networks on the way to their destination. Malek-Madani, *supra* at 5. A server is a "computer which provides services to other computers on a network," such as a "computer where a website is located." *Id.* Servers are often housed in large data centers, spaces "dedicated to housing computer systems or telecommunications infrastructure." *Id.*

[4] *Id.* at 4.

and networks that enable their transactions. Without having to understand the internet's underlying technical complexities, the internet can be accessible to a wide audience of ages and technical proficiencies. Internet infrastructure, at its best, makes internet transactions seem simple, immediate, and reliable, fostering user confidence and encouraging widespread adoption of globally transformative internet technologies. Ultimately, the hidden nature of the internet's inner workings is crucial to its value—the ability to provide instant and seamless access to vast amounts of information and services worldwide, with little effort or technical knowledge required.

For all users might know, the infrastructural components involved in their online transactions could be physically located anywhere in the world. However, data is especially likely to pass through servers in the U.S., due to the concentration of major technology companies and infrastructure here. The U.S. has, by far, the most data centers in the world.[5]

---

[5] *See* Brian Daigle, *Data Centers Around the World: A Quick Look*, United States International Trade Commission (May 2021), https://www.usitc.gov/publications/332/executive_briefings/ebot_data_centers_around_the_world.pdf (over 2,600 data centers in the U.S. in 2021, with the U.S. housing 33% of the world's data centers); Miranda S. Spivack, *More Data in the Cloud Means More Centers on the Ground to Move It*, N.Y. Times (June 27, 2023) https://www.nytimes.com/2023/06/27/business/data-centers-internet-infrastructure-development.html (2,701 data centers in the U.S. in 2022 with Germany in a "distant second"); John Minnix, *115 Data Center Stats You Should Know in 2024*, Brightlio (Apr. 22, 2024, https://brightlio.com/data-center-

Many of the world's largest "data producing and data consuming" companies, such as Google, Amazon, Meta, and Microsoft, are based in the U.S. and maintain data centers here.[6] Up to 70% of the world's internet traffic passes through servers in data centers in Northern Virginia, in the town of Ashburn, in Loudoun County—referred to as "Data Center Alley."[7] "Pretty much any email sent or received anywhere around the globe, comes through this town. If you've got something stored in the cloud, it's probably in one of the 100-plus data centers located in Loudoun County."[8] A "similar hub lies near Silicon Valley" in California, and ultimately, "[a] majority of the world's internet traffic flows through the sites in these two regions, which function as crucial internet conveyor belts."[9]

Internet users almost never have knowledge or control over where their data is geographically located, or the physical locations of the servers and routers that carry the signals they send. The internet only works because most people don't have to know or care how it works.

---

stats/ (5,388 data centers in the U.S. in 2024 based on various sources).

6 Daigle, *supra*.

7 Dora Mekouar, *Here's Where the Internet Actually Lives*, VOA (Feb. 17, 2020), https://www.voanews.com/a/usa_all-about-america_heres-where-internet-actually-lives/6184090.html/.

8 *Id.*

9 Spivack, *supra*.

II. HOW BLOCKCHAIN TRANSACTIONS WORK

The description of the internet set forth above is the internet commonly used today to send emails, order books online, order food delivery, or access social media websites. Most of the companies that provide these services—Google for email, Amazon for books, Seamless for food delivery, Meta or Reddit for social media—are centralized companies that conduct their internet transactions on servers of their choosing. They may not choose all the routers or servers in the network chains between the companies and their users, but they have some control.

Blockchain-based architecture works differently. Blockchains are the new internet infrastructure; they are blocks of data that are linked into a digital chain. Each "block" is a ledger that is updated and added to with permanently recorded data. This information is stored in a distributed or "decentralized" system, where each block's data is confirmable by every participating computer on that blockchain network.[10]

There is no centralized control over a blockchain. Rather, copies of all information and transactions on a blockchain are distributed across the blockchain network. When a transaction is added to this system, sometimes called a "distributed ledger," it is

---

[10] *See* Stanford Engineering Center for Global & Online Education, *How Does Blockchain Work?*, https://online.stanford.edu/how-does-blockchain-work (last visited Oct. 24, 2024).

synced with every node of the blockchain, regardless of the physical geography of those nodes.[11]

No one entity, organization, person, or group of persons is necessary to operate a blockchain, or to facilitate or allow access to users interacting directly with the blockchain. While some companies may use private blockchains that they entirely control, most public blockchains operate autonomously, *i.e.*, no people or entities need to coordinate consciously for them to run, and "permissionlessly," *i.e.*, no one needs authorization to interact with the blockchain directly.[12]

The decentralized nature of blockchain technology also has promoted competition within the various layers of internet infrastructure. Due to the lower barriers to entry associated with blockchain technology, a wider and more diverse array of developers can build internet products and services.[13]

A blockchain has different types of "nodes," typically computers or devices, that participate to perform different functions. Two common types are "validator" or "miner" nodes, which help secure and process the transactions on a blockchain. In a proof-

---

[11] *Id.*

[12] *Id.*

[13] *See* Miles Jennings, *Why Decentralization Matters, for Builders*, a16zcrypto (June 24, 2024), https://a16zcrypto.com/posts/article/why-decentralization-matters-builders/.

of-work consensus process (such as for the Bitcoin blockchain), miners complete a mathematical puzzle, which adds blocks to the chain and mines new coins. In a proof-of-stake consensus mechanism (such as for the modern Ethereum blockchain), nodes in a blockchain network use an algorithm to agree on the next valid block of transactions that will be added to the blockchain.[14]

A validator is a participant in a proof-of-stake blockchain running a computer that verifies the transactions on the network. To become a validator, a network participant can choose to "stake" (or "put up") a specific amount of the network's native token, but no agreement or permission is required for a participant to become a validator in a proof-of-stake blockchain. Blockchain networks can have hundreds or thousands of nodes. The Ethereum blockchain, for example, has over one million validators.[15] The validator nodes across the full blockchain industry span the globe, and for the most part, they do not coordinate, work together, or even know each other. Indeed, anyone can undertake blockchain node deployment, on their own or through commercially-available services.[16] The

---

[14] *How Does Blockchain Work?*, *supra.*

[15] Zoltan Vardai, *Ethereum Validators up 30% in a Year, Driven by Institutional Adoption*, Cointelegraph (Oct. 16. 2024), https://cointelegraph.com/news/ethereum-validators-up-30-year-institutional-adoption.

[16] *See, e.g.*, Ian Holtz, *et al.*, *Blockchain Node Deployment on AWS: A Comprehensive Guide*, AWS Database Blog (Apr. 29, 2024), https://aws.amazon.com/blogs/database/blockchain-node-deployment-on-aws-a-comprehensive-guide/.

widespread deployment of nodes around the world has numerous benefits: enhancing the resiliency and security of networks, maintaining integrity by allowing for independent verification of blockchain transactions, preventing a single "point of failure" in the event of an outage in one area, and promoting transparency because validators can verify transactions from a node anywhere.

Due to the dispersed nature of blockchains and the large number of nodes it takes to operate them, knowing where all the nodes on a particular chain are physically located is difficult, and sometimes impossible. Most users of a blockchain network, as well as users of applications or networks that are built and operate on top of blockchain networks, do not and cannot know where any given node is located, much less all the nodes. It would be nearly impossible to know in advance which of the hundreds or thousands of validators on a blockchain network would be the requisite "majority" that validated a particular transaction at a particular time.

Luckily, knowing where nodes are located is irrelevant—users do not need to know or understand where nodes are located to use or participate in a blockchain network, much in the same way that typical internet users do not need to know or understand internet infrastructure, or where servers are located, to access the internet seamlessly. For the average user, the invisibility of blockchain architecture resembles the invisibility of other modern internet architecture. The fact that users do not care about (and are unaware of) the

location of nodes underscores the error in the Second Circuit's decision and the dangerous consequences resulting therefrom.

III. USE CASES OF BLOCKCHAIN INFRASTRUCTURE

Due to the dispersed nature of the nodes that secure a blockchain, and the distributed ledger that records data immutably, blockchain infrastructure carries strong advantages for cybersecurity, transparency, traceability, automation, and recordkeeping. When hundreds or thousands of computers across the globe are securing the data separately, tampering with a blockchain is much more difficult—there is no one "point of failure" that can destroy an entire network, and by creating records that cannot be altered (and can be encrypted), blockchain technology can help prevent fraud. It is no surprise that blockchain networks are rising as back-office technology, both in "private blockchains" (controlled entirely by one party or a limited number of parties), or "public blockchains" (open for anyone in the world to use without any permission).[17]

Companies and even countries around the globe integrate and rely on blockchain infrastructure to capitalize on the benefits of decentralization, such as

---

[17] *See generally The Value Prop*, Polygon, https://thevalueprop.io/ (last visited Oct. 24, 2024). TheValueProp is an internet database that features numerous blockchain use cases across many verticals, including sustainability, humanitarian work, education, and others.

the ease of access and permissionless nature of the underlying technology.

These benefits are illustrated by the many traditional finance companies moving into blockchain. For example, Franklin Templeton offers a tokenized money market fund that uses a public blockchain to process transactions and record share ownership,[18] and announced that shares of the fund can be transferred on a blockchain.[19] BlackRock and UBS offer tokenized money market funds on Ethereum.[20] Multiple traditional finance firms offer Bitcoin and Ethereum "exchange traded products."[21]

---

[18] Lyllah Ledesma, *A $1.4T Financial Giant Expands Its Money Market Fund on Polygon*, CoinDesk (Apr. 26, 2023), https://www.coindesk.com/business/2023/04/26/a-14t-financial-giant-expands-its-money-market-fund-on-polygon.

[19] Franklin Templeton, *Franklin Templeton Announces Availability of Peer-to-Peer Transfers for Franklin OnChain U.S. Government Money Fund* (Apr. 25, 2024), https://www.franklintempleton.com/press-releases/news-room/2024/franklin-templeton-announces-availability-of-peer-to-peer-transfers-for-franklin-onchain-u.s.-government-money-fund.

[20] Krisztian Sandor, *BlackRock's BUIDL Becomes Largest Tokenized Treasury Fund Hitting $375M, Toppling Franklin Templeton's*, CoinDesk (Apr. 30, 2024), https://www.coindesk.com/markets/2024/04/30/blackrocks-buidl-becomes-largest-tokenized-treasury-fund-hitting-375m-toppling-franklin-templetons/; Ezra Reguerra, *Swiss Bank UBS Launches Tokenized Money Market Fund on Ethereum*, Cointelegraph (Oct. 2, 2023), https://cointelegraph.com/news/ethereum-ubs-tokenize-money-market-fund-launch.

[21] *Bitcoin ETFs List*, VettaFi (Oct. 24, 2024), https://etfdb.com/themes/bitcoin-etfs/; *Ethereum ETFs List*,

Hamilton Lane launched a private credit fund on the Solana blockchain.[22] PayPal permits users to transfer cryptocurrency to other users.[23] BNY Mellon announced that it would accept cryptocurrency deposits from retail users, just like it accepts fiat currency.[24] Traditional finance firms are also experimenting with private blockchains, further cementing the practical use of blockchain technology.[25]

VettaFi, https://etfdb.com/themes/ethereum-etfs/ (last visited Oct. 24, 2024).

[22] Niamh Rowe, *Hamilton Lane Becomes First Asset Manager to Launch a Fund on Solana Blockchain*, yahoo!finance (July 23, 2024), https://ca.finance.yahoo.com/news/hamilton-lane-becomes-first-asset-100000656.html.

[23] *PayPal Users Can Now Transfer, Send, and Receive Bitcoin, Ethereum, Bitcoin Cash, and Litecoin*, PayPal (Aug. 12, 2022), https://newsroom.paypal-corp.com/2022-06-07-PayPal-Users-Can-Now-Transfer-Send-and-Receive-Bitcoin-Ethereum-Bitcoin-Cash-and-Litecoin.

[24] Mehnaz Yasmin and Saeed Azhar, *BNY Mellon to Offer Crypto Services in Digital Asset Push*, yahoo!finance (Oct. 11, 2022), https://finance.yahoo.com/news/bny-mellon-offer-crypto-services-143413827.html.

[25] *See* Oliver Knight, *Wall Street Giant DTCC Launches Private Blockchain in Big Crypto-Milestone for TradFi*, CoinDesk (Aug. 22, 2022), https://www.coindesk.com/business/2022/08/22/wall-streets-dtcc-launches-private-blockchain-platform-to-settle-trades (DTCC is testing the use of a private blockchain for settlement and clearing); Businesswire, *Citi Develops New Digital Asset Capabilities for Institutional Clients* (Sept. 18, 2023), https://www.businesswire.com/news/home/20230918024720/en/Citi-Develops-New-Digital-Asset-Capabilities-for-Institutional-Clients (Citibank is offering "blockchain and

Many non-financial companies are also using blockchain technologies, including Google,[26] AMC Theatres,[27] Subway,[28] and Starbucks.[29] Blockchain infrastructure is being used to build decentralized online cloud storage, and is considered a pivotal network feature because servers are managed by independent and diverse entities across the world.[30] Decentralized blockchain-based networks are using

---

smart contract technologies to deliver digital asset solutions for institutional clients").

[26] Oliver Knight, *Google Partners With Coinbase to Accept Crypto Payments for Cloud Services*, yahoo!finance (Oct. 11, 2022), https://ca.finance.yahoo.com/news/google-partners-coinbase-accept-crypto-121803385.html.

[27] Chris Katje, *AMC To Accept Bitcoin and Crypto For Payment, Are NFT Commemorative Tickets Next?*, yahoo!finance (Sept. 19, 2021), https://finance.yahoo.com/news/amc-accept-bitcoin-crypto-payment-205509000.html.

[28] Andrew Torba, *I Bought Subway with Bitcoin and it was Awesome*, Coindesk (April 9, 2024), https://www.coindesk.com/business/2013/11/22/i-bought-subway-with-bitcoin-and-it-was-awesome/.

[29] Samyuktha Sriram, *Customers Can Reload Starbucks Card With Bitcoin and Ethereum As Coffeehouse Explores 'Tokenizing Stars,'* yahoo!finance (Nov. 11, 2021), https://finance.yahoo.com/news/customers-reload-starbucks-card-bitcoin-154130368.html.

[30] Max (Chong) Li, *Why Blockchain is Necessary in Decentralized Clouds*, Forbes (Sept. 30, 2023), https://www.forbes.com/sites/digital-assets/2023/09/30/why-blockchain-is-necessary-in-decentralized-clouds/.

nodes as hotspots to connect wireless devices to the internet.[31]

Other countries have recognized the importance of blockchain infrastructure.[32] Many countries are promulgating relevant regulatory frameworks, including (among others) the European Union, the U.K., Switzerland, the United Arab Emirates, Hong Kong, Singapore, Japan, South Korea, the Cayman Islands, and the British Virgin Islands.[33] Finland's

---

[31] Andrew Hayward, *Andreessen-Backed Helium Raises $111 Million to Grow Crypto Wireless Network*, Decrypt (Aug. 10, 2021), https://decrypt.co/78222/andreessen-backed-helium-raises-111-million-to-grow-crypto-wireless-network.

[32] Andrey Sergeenkov, *China Bets on Massive Blockchain Infrastructure*, Forbes (Oct. 10, 2024), https://www.forbes.com/sites/digital-assets/2024/10/08/china-bets-on-massive-blockchain-infrastructure/.

[33] *See* Jack Schickler, *MiCA, EU's Comprehensive New Crypto Regulation, Explained*, CoinDesk (Sept. 7, 2023), https://www.coindesk.com/learn/mica-eus-comprehensive-new-crypto-regulation-explained; Ryan Browne, *UK Confirms Plans to Regulate Crypto Industry with Formal Legislation*, CNBC (Oct. 30, 2023), https://www.cnbc.com/2023/10/30/uk-confirms-plans-to-regulate-crypto-industry-with-formal-legislation.html; Jeff Wilser, *Zug: Where Ethereum was Born and Crypto Goes to Grow Up*, CoinDesk (June 27, 2023), https://tinyurl.com/yc7nemby; Dillin Massand, *Dubai: Launching a Crypto Regulatory Arm to Become a Global Financial Power*, CoinDesk (June 27, 2023), https://www.coindesk.com/consensus-magazine/2023/06/27/dubai-launching-a-crypto-regulatory-arm-to-become-a-global-financial-power/; Sebastian Widmann, *How The UAE Became a Crypto Hub Poised for Explosive Growth*, Forbes (Nov. 16, 2023), https://www.forbes.com/sites/digital-assets/2023/11/16/how-the-uae-became-a-crypto-hub-poised-for-explosive-growth;

tax administration has begun integrating blockchain to track real estate transactions.[34] Brazil developed a blockchain network to increase security around data sharing as it implements a new national identity card.[35]

These examples—particularly those using public blockchains—demonstrate the use of blockchain networks that automatically rely on nodes around the globe, without any one or any company verifying where the nodes are for the businesses or initiatives to operate. If companies had to identify where nodes that verify transactions are located, for the purpose of assessing their jurisdictional reach and perhaps even to "opt out" of specific jurisdictions' bodies of law—even if that were possible—it would derail not

---

Katherine Ross & Jack Kubinec, *Hong Kong to Create Regulatory Regime for Stablecoin Issuers*, Blockworks (Dec. 27, 2023), https://blockworks.co/news/hong-kong-stablecoin-regulation; Emily Parker, *How Japan Is Leading the Race to Regulate Stablecoins*, CoinDesk (Oct. 25, 2023), https://tinyurl.com/5ev34sth; Danny Park, *South Korea's Inaugural Crypto Law Goes Into Full Effect*, The Block (July 19, 2024), https://tinyurl.com/yjrnbkpj; Virtual Asset (Service Providers) Act (2022 Revision), (Jan. 31, 2022) (Cayman Is.), https://tinyurl.com/3x7e97cb.

[34] Alfredo Collosa, *How Global Tax Administrations Are Using Blockchain Technology*, Bloomberg Tax (Mar. 17, 2022), https://news.bloombergtax.com/daily-tax-report-international/how-global-tax-administrations-are-using-blockchain-technology.

[35] Angelica Mari, *Brazil Develops Blockchain Network to Support ID Rollout*, Forbes (Sept. 28, 2023), https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-develops-blockchain-network-to-support-id-rollout/.

just U.S.-based blockchain infrastructure, but entire businesses and business initiatives.

ARGUMENT

I. THE SECOND CIRCUIT'S DECISION IS AT ODDS WITH *MORRISON*'S TEACHINGS IN THE CONTEXT OF THE SECURITIES ACT AND EXCHANGE ACT

The Second Circuit's holding in this case implicates the Securities Act of 1933 (15 U.S.C. § 77) and the Securities Exchange Act of 1934 (15 U.S.C. § 78). These statutes animated the *Morrison* decision in the first place, as this Court was wary of allowing U.S. courts to become "the Shangri-La of class action litigation for lawyers representing those allegedly cheated in foreign securities markets." 561 U.S. at 270.

The Second Circuit's decision ignores the teaching of *Morrison*. Using internet infrastructure, over which users would have no choice or control, would reduce the doctrine of extraterritoriality to (as this Court described it) a "muzzled Chihuahua." *Abitron Austria GmbH v. Hetronic Int'l, Inc.*, 600 U.S. 412, 426 (2023).

Long gone are the days of open-outcry trading pits on the floor of the New York Stock Exchange. In the modern financial world, virtually all securities transactions take place over the internet, and orders are routed through servers, routers, and wiring around the world.

While the Second Circuit has wrestled with where modern securities transactions take place, it did not previously find the location of internet infrastructure to be relevant. Before its decision in this case, the Second Circuit focused on where the human beings, not computer servers, were located. *See, e.g.*, *Choi v. Tower Research Cap. LLC*, 890 F.3d 60, 67-68 (2d Cir. 2018) (irrevocable liability attached in the U.S. because persons directed trades to be matched through a domestic exchange); *Giunta v. Dingman*, 893 F.3d 73, 80-81 (2d Cir. 2018) (irrevocable liability occurred in New York because parties met there, one party received communications there, and funds were transferred from there); *Fed. Hous. Fin. Agency v. Nomura Holding Am., Inc.*, 873 F.3d 85, 156–58 (2d Cir. 2017) (irrevocable liability attached in D.C. and Virginia because agency employees worked there and received emailed offer materials there); *United States v. Vilar*, 729 F.3d 62, 76–78 (2d Cir. 2013) (irrevocable liability hinged on location where party executed documents, and location from where money was sent); *Absolute Activist Value Master Fund Ltd. v. Ficeto*, 677 F.3d 60, 62 (2d Cir. 2012) (parties who never resided in the U.S. and transactions not alleged to have occurred in the U.S. not sufficiently alleged to be domestic).

If the location of internet infrastructure were relevant, virtually any court examining *Morrison* could conclude the transaction was domestic, for the simple fact that the U.S. is far and away the world leader in internet infrastructure. Securities transactions, even between non-U.S. parties, may

easily use American internet infrastructure, without either party even knowing it. *Morrison* would be greatly diminished if "lawyers representing those allegedly cheated in foreign securities markets" were able to point to these intermediary infrastructural touchpoints as grounds for the "domesticity" of a transaction. *Morrison*, 561 U.S. at 270. If "the mere placement of a buy order in the United States for the purchase of foreign securities on a foreign exchange" was insufficient to allege that a purchaser incurred irrevocable liability in the U.S., *City of Pontiac Policemen's & Firemen's Retirement Systems v. UBS AG*, 752 F.3d 173, 181 (2d Cir. 2014), then the incidental fact that the buy order settled on a server in the U.S., unbeknownst to that buyer, could not possibly suffice. Yet here, the Second Circuit concluded otherwise.

This issue becomes more acute in the blockchain transaction world, where internet infrastructure, such as the machine where orders are matched, is not even necessarily housed on one machine in one location—but instead, is located on every server node on the blockchain, everywhere around the world. If the location of "settlement" on a blockchain were relevant, then *Morrison* retreats to its kennel, a craven watchdog, as virtually every blockchain transaction could be said to have settled, at least in part, on nodes located in the U.S.

Morrison rejected the notion that all transactions should or can feasibly be subject to litigation in the U.S. The Second Circuit's decision would result in exactly that, providing a basis to subject all securities transactions (and other conduct

potentially subject to U.S. law, *see infra* at Section II) to litigation in the U.S.—a result that could overwhelm the judicial system and undermine the presumption against extraterritorial application of U.S. law.

II. THE SECOND CIRCUIT'S DECISION IMPLICATES ALL FEDERAL LAWS

As *Morrison* makes clear, the doctrine of extraterritoriality is broader than just the Securities Act and the Exchange Act. It applies to all "legislation of Congress." 561 U.S. at 255 (citations omitted). The Second Circuit improperly looked to the location of internet infrastructure to conclude that *Morrison* did not bar claims under the Securities Act and the Exchange Act. But the Second Circuit rule, if allowed to stand, would apply to all federal statutes, leading to an evisceration of the *Morrison* doctrine in many areas of federal law. Internet usage is now universal, constant, and often international, and thus is implicated in many cases, under many different federal statutes, that might have come out differently under the Second Circuit rule. For example:

– In *Loginovskaya v. Batratchenko*, 764 F.3d 266, 271–74 (2d Cir. 2014), the Second Circuit upheld the dismissal of a case brought under the Commodities Exchange Act because it was based on extraterritorial commodities transactions where the plaintiff wired funds to a bank in New York, necessarily implicating the banks' internet infrastructure in the U.S.

– In *Sexual Minorities Uganda v. Lively*, 254 F. Supp. 3d 262, 268 (D. Mass. 2017), the court dismissed a case brought under the Alien Tort Statute on extraterritoriality grounds where the defendant resided in the U.S. and sent emails originating from the U.S. in connection with crimes in Uganda. The use of internet infrastructure was insufficient to invoke domesticity.

– In *IMAPizza, LLC v. At Pizza Ltd.*, 334 F. Supp. 3d 95, 118 (D.D.C. 2018), *aff'd* 965 F.3d 871, 879 (D.C. Cir. 2020), defendant's travel to the U.S., taking pictures during those visits, and downloading "copyrighted pictures from U.S. servers" was not sufficiently domestic activity to constitute a violation of the Copyright Act.

– In *Hourani v. Mirtchev*, 943 F. Supp. 2d 159, 167 (D.D.C. 2013), *Cedeño v. Intech Grp., Inc.*, 733 F. Supp. 2d 471, 473 (S.D.N.Y. 2010), courts dismissed cases where money laundering through domestic banks—necessarily implicating the banks' internet infrastructure in the U.S.—was insufficient to justify extraterritorial applications of the Racketeer Influenced and Corrupt Organizations Act ("RICO"). Similarly, in *Sonterra Capital Master Fund Ltd. v. Credit Suisse Grp. AG*, 277 F. Supp. 3d 521, 581 (2017), a RICO claim was dismissed on *Morrison* grounds, even though defendants purportedly caused manipulated interest rate information "to be published to servers in the United States and used United States wires to memorialize trades affected by that rate."

– In *Nakhid v. Am. Univ.*, No. 19-cv-3268 (APM), 2021 WL 4169355, at *6 (D.D.C. Sept. 14, 2021), the court dismissed claims under the Civil Rights Act of 1964 and 42 U.S.C. § 1981 for being impermissibly non-domestic, even though job descriptions were posted online for an American University coaching position.

As a result, the implications of the Second Circuit's decision are far greater than just securities laws. The Second Circuit's decision, if left to stand, could be cited in cases brought under any federal statute. And given the international interconnectedness of internet infrastructure, with much of it located in the U.S., *Morrison* would be eviscerated.

III. THE SECOND CIRCUIT DECISION HAMPERS INTERNET TRANSACTIONS GENERALLY, AND BLOCKCHAIN TRANSACTIONS IN PARTICULAR

If using U.S. internet infrastructure implicated U.S. jurisdiction for any federal laws, beyond just running afoul of *Morrison*, multiple harms would result.

First, foreign companies, across industries, would terminate use of U.S. internet infrastructure. If a foreign company knew that using an American component of internet infrastructure were sufficient grounds to be sued in the U.S., under U.S. laws, they would grow far more cautious about ensuring that any internet traffic they routed, or servers they used, were outside the U.S. American data center

companies, such as AWS, Microsoft, Google, Meta, and many others, would lose significant business to non-American providers (such as the U.K.'s Equinix or Digital Realty, Japan's NTT, China's GDS Holdings, or Europe's Telehouse), as companies outside the U.S. seek to ensure that their data never touched the U.S. in any way. Worse, there would be a "network effect," as other infrastructure companies that exclusively connect through these American giants would have to find alternative, foreign, providers. These impacts would severely diminish American leadership in the internet world—including, for example, shifting more internet activity offshore, making it more difficult for U.S. law enforcement to halt illicit finance and protect American consumers.

Second, the principles of comity in the internet era would be eroded, and U.S. citizens would be in greater danger of being haled into foreign courts, and subject to foreign law, because of the happenstance of the internet infrastructure used in their transactions. If foreign companies could be sued in the U.S. (and under U.S. laws) just for using American internet infrastructure, other countries may adopt the same principles. An American violating a Chinese law against certain types of political speech, where that comment was housed on a Chinese server, could be sued in China for that action—even if the user had absolutely no idea that the comment touched any Chinese internet infrastructure.

The Second Circuit sought to avoid this parade of horribles with an "exception" tailor-made to distinguish this particular case. It reasoned that Binance "notoriously denies the applicability of any other country's securities regulation regime," so there was no need to show comity to another country. Pet'r's App. 17a. The Second Circuit allowed that its "conclusion might be different were we faced with plaintiffs seeking to apply U.S. securities laws based on the happenstance that a transaction was initially processed through servers located in the U.S. despite all parties to the transaction understanding that they were conducting business on a foreign-registered exchange." Pet'r's App. 16a-17a.

That "exception" is not workable in typical internet transactions, and impossible in blockchain transactions. In a typical internet transaction, "all parties to the transaction" would not necessarily have any idea that they are "conducting business on a foreign-registered exchange" (or other business). As illustrated above, most users have little idea where their data passes through, nor should they. An allegation that some back-office processing equipment happened to be in the U.S. should not be sufficient to drag the entire matter into U.S. court under U.S. law. After all, the relevant portion of the Second Circuit's decision did not focus on Binance's alleged conduct, so much as the geographical location of a third party, AWS. *Cf.* Pet'r's Br. 20-21.

To go a step further, any transaction processed on a digital asset exchange is, at heart, a blockchain

transaction. Any blockchain transaction would be processed on all of the nodes on that chain, all over the world. Binance allegedly "matched" orders on AWS, but to publish that transaction onto the blockchain requires a worldwide network of transactions, in geographic locations that would be impossible for users to know about. If the U.S. could exercise jurisdiction over a digital assets exchange for using AWS, then any country in the world using the same rule could exercise jurisdiction over an American for using any public blockchain. Such a rule would be offensive to comity, and destructive of the advantages that a worldwide internet, and worldwide blockchain accessibility, can provide. It would risk splintering the next iterations of the internet into national fortresses, to the poverty of the world.

Variants of the Second Circuit's reasoning have already appeared in lower courts across the country. *See, e.g.*, *SEC v. Scoville*, 913 F.3d 1204, 1219 (10th Cir. 2019), *cert denied*, 140 S. Ct. 483 (2019) ("We add that the servers housing the Traffic Monsoon website were physically located in the United States."); *SEC v. Balina*, No. 22-cv-00950 (DAE), 2024 WL 2332965, at *8 (W.D. Tex. May 22, 2024) (use of U.S.-based social media platforms constituted sufficient U.S. activity); *Williams v. Block One*, No. 20-cv-2809 (LAK), 2022 WL 5294189, at *7 (S.D.N.Y. Aug. 15, 2022) ("the location of the node that verified the specific transaction at issue should control in this circuit under *Morrison*'s second prong as construed in *Absolute Activist*."); *In re Tezos Sec. Litig.*, No. 17-cv-06779-RS, 2018 WL

4293341, at *8 (N.D. Cal. Aug. 7, 2018) (use of server in Arizona was a factor to defeat extraterritoriality). These cases, improperly pointing to the use of U.S. internet infrastructure to exercise jurisdiction, will continue to put *Morrison* back in its kennel, unless stopped.[36]

This case presents a remarkably clean vehicle for the Supreme Court to put an end to the lower courts' erosion of the *Morrison* doctrine, and to pave the digital roads of the future. CCI stands for the promotion of blockchain technology in the U.S. and around the world. The Second Circuit's decision risks splintering the global nature of the internet, and more acutely, hampering the development of the next generation of internet-based technologies, in turn devastating entire industries.

---

[36] This issue goes beyond court decisions. Administrative agencies use judicial precedents, especially circuit court precedents, as leverage to negotiate settlements. Given that far more agency actions are settled than litigated, and agencies can bring tremendous pressure to settle, it is even more critical to correct the Second Circuit's error.

CONCLUSION

For the foregoing reasons, the Court should grant the petition.

Respectfully submitted,

Jason P. Gottlieb
Counsel of Record
Daniel C. Isaacs
Michael Mix
Rachel Fleder
Vani Upadhyaya
MORRISON COHEN LLP
909 Third Avenue
New York, New York 10022
(212) 735-8600
jgottlieb@morrisoncohen.com

Counsel for Amicus Curiae The Crypto Council for Innovation

October 25, 2024