No. 23-50669

IN THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

JOSEPH VAN LOON, ET AL.,
Plaintiffs-Appellants,

v.

DEPARTMENT OF TREASURY, ET AL.,
Defendants-Appellees.

BRIEF FOR THE DEFI EDUCATION FUND AS AMICUS CURIAE IN SUPPORT OF APPELLANTS AND REVERSAL

J. Abraham Sutherland
106 Connally Street
Black Mountain, NC 28711
(805) 689-4577

Cameron T. Norris
Jeffrey S. Hetzel
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Ste. 700
Arlington, VA 22209
(703) 243-9423
cam@consovoymccarthy.com

Counsel for Amicus Curiae DeFi Education Fund

CERTIFICATE OF INTERESTED PERSONS

Per Circuit Rule 28.2.1, the DeFi Education Fund certifies that—in addition to the persons listed on the certificate of interested persons submitted by Appellants—the following listed persons have an interest in the outcome of this case. These representations are made in order for the judges of this Court to evaluate possible disqualification or recusal.

1. DeFi Education Fund, *Amicus Curiae*
2. Cameron T. Norris, Counsel for *Amicus Curiae*
3. Consovoy McCarthy PLLC, Counsel for *Amicus Curiae*
4. J. Abraham Sutherland, Counsel for *Amicus Curiae*
5. Jeffrey S. Hetzel, Counsel for *Amicus Curiae*

Dated: November 20, 2023 */s/ Cameron T. Norris*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Regulations & Executive Orders

Legislative Documents

Other Authorities

INTEREST OF AMICUS CURIAE[1]

DeFi Education Fund is a nonpartisan research and advocacy group based in the United States. DEF's mission is to explain the benefits of decentralized finance, achieve regulatory clarity for decentralized finance technology, and realize the transformative potential of decentralized finance for everyone. DEF advocates for decentralized finance users, participants, and software developers working to create new decentralized finance products using blockchain technology. Among other things, DEF educates the public about decentralized finance through weekly newsletters, op-eds, podcasts, and print media; meets with members of Congress to discuss decentralized finance and related issues; and submits public comments on proposed rulemakings that impact decentralized finance.

Decentralized finance is part of the cryptocurrency ecosystem. DEF has an interest in educating courts about the nature of these vital technologies and how cryptocurrency works. And it has an interest in protecting the rights of cryptocurrency users to develop and use software tools, like the one at issue here, that let them use cryptocurrency securely and privately.

---

[1] In accordance with Federal Rule of Appellate Procedure 29(a)(4)(E), DEF certifies that this brief was authored by DEF's counsel and that no party or counsel for any party funded the preparation or submission of this brief. All parties have consented to the filing of this amicus brief.

INTRODUCTION & SUMMARY OF THE ARGUMENT

This case is about agency overreach. The International Emergency Economic Powers Act authorizes the executive branch to regulate certain foreign transactions, but not wholly domestic transactions. Here, the Office of Foreign Assets Control invoked IEEPA to regulate certain domestic cryptocurrency transactions. OFAC made it a federal felony for Americans to use a software tool that allows them to make cryptocurrency transactions privately, even when their use of that software tool does not involve any foreigners or their property interests. OFAC thereby exceeded its statutory authority to regulate transactions involving "property in which foreign[ers] have any interest." *See* 50 U.S.C. §1702(a)(1)(B). The district court's decision upholding OFAC's action failed to enforce this crucial limitation.

I. IEEPA's limits are real. "The grant of authorities in IEEPA does *not* include the power to ... regulate purely domestic transactions." *Regan v. Wald*, 468 U.S. 222, 228 n.8 (1984) (emphasis added). IEEPA's plain text limits the executive to regulating transactions involving "property in which any foreign country or a national thereof has any interest." 50 U.S.C. §1702(a)(1)(B). IEEPA's history demonstrates that Congress did not want the executive to regulate domestic transactions. It deliberately removed language that had previously authorized such regulation. And Supreme Court precedent requires the executive, before regulating any transaction under IEEPA, to demonstrate that foreigners have a property interest—defined by positive property law—in that transaction. *Dames & Moore v. Regan*, 453 U.S. 654, 675-77 (1981).

II. Here, however, OFAC criminalized certain "purely domestic transactions." *Wald*, 468 U.S. at 228 n.8. It banned Americans from using a software tool to protect their own crypto assets without moving them to another person or entity. In the course of these now-banned transactions, these Americans would not give anything to any foreigner. They would not take anything from any foreigner. And their assets would not be controlled by any foreigner. The now-banned transactions would include not only purely domestic but even solitary uses of software. The district court's observation that Americans *could* use the banned software tool to transact with foreigners—through the use of an optional feature called a "relayer"—does not absolve OFAC of its overreach in regulating domestic transactions. It underscores it: All domestic transactions could be foreign if you added a foreigner.

Likewise, the district court's observation that people colloquially call code a "smart contract" does not make the software tool a *legal* contract, let alone one in which foreign individuals have a property interest. The district court said without authority that the code constituted a legal contract because it "provide[d] Tornado Cash with a means to control and use crypto assets" but cited no support for that proposition and no basis for concluding that using the software tool creates a legal contract involving foreigners. *See* ROA.1496, 1510 (citing nothing).

The district court finally resorted to giving the agencies an "even greater degree of deference" than under *Chevron* and *Auer* combined. ROA.1505. But because this case involves an interpretation of a statute carrying criminal penalties, this Court's precedent

makes clear that all deference is due to the challengers. *Cargill v. Garland*, 57 F.4th 447, 466 (5th Cir. 2023) (en banc), *cert. granted*, 2023 WL 7266996 (Nov. 3, 2023). And OFAC's in-litigation interpretations of its own regulations are not entitled to deference under *Kisor v. Wilkie*, 139 S. Ct. 2400, 2414-18 (2019), which the district court did not consider.

III. The software tool that OFAC banned is important. Responsible Americans used it regularly to protect their privacy when using cryptocurrency. There is nothing inherently illicit in the desire for financial privacy. Unlike other economic activities, cryptocurrency transactions are posted to a public ledger that anyone can see, which allows their transactions to be viewed by anyone with access to the internet if their identity is connected to any one transaction. That unique feature can create major privacy concerns that can expose individuals to exploitation, invite retaliation for politically-sensitive contributions, and leave users' private and sensitive affairs exposed to everyone. The software tool that OFAC banned solved these problems by empowering users to preserve their own privacy in these public transactions. OFAC's overreach therefore harms ordinary Americans who want to use cryptocurrency responsibly.

The Court should reverse so that OFAC can craft a narrower and appropriately tailored designation that satisfies its concerns regarding foreigners but complies with IEEPA.

ARGUMENT

I. OFAC is not allowed to ban Americans' domestic transactions.

This case turns on whether OFAC's ban on Americans using software falls within the scope of the International Emergency Economic Powers Act of 1977. IEEPA gives the President power over international affairs. He can prohibit, if certain conditions are met, a range of activities involving *foreigners'* property interests. Specifically, he can regulate or prohibit:

> any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving,
>
> **any property in which any foreign country or a national thereof has any interest**
>
> by any person, or with respect to any property, subject to the jurisdiction of the United States

50 U.S.C. §1702(a)(1)(B) (breaks and emphasis added). IEEPA's crucial requirement is the second clause, which limits the President's authority to activities involving "property in which any foreign[er] has any interest." That clause prevents the President from regulating wholly domestic transactions.

Other laws do not expand the scope of this second clause. The North Korea Sanctions and Policy Enhancement Act of 2016 makes the exercise of this power mandatory to block aid to North Korean weapons activities. 22 U.S.C. §9214(a), (c). And two executive orders create emergencies that satisfy one of IEEPA's preconditions so that OFAC can exercise this power with respect to North Korea and cyber-related threats. 80 Fed. Reg. 18,077; 81 Fed. Reg. 14,943. All agree that, for OFAC's action to

be upheld here, it must satisfy the requirement in IEEPA's second clause—*i.e.*, it must regulate only activities involving foreigners' property interests.

IEEPA's history is crucial to understanding that clause. In 1917, Congress said the President could prohibit certain transactions in emergencies, but only transactions "between the United States and any *foreign country*." Trading with the Enemies Act, Pub. L. 65-91 §5(b), 40 Stat. 411, 415 (1917) (emphasis added). Congress would not allow the President to regulate "transactions to be executed wholly within the United States." *Id.*; *see also* H.R. Rep. 95-495, at 4 (1977); *Report of the Special Committee on the Termination of the National Emergency*, S. Rep. No. 93-549, at 185 (1973). But in 1933, to authorize an emergency bank holiday in the frenzy of the Great Depression, Congress expanded the Act to allow regulation of domestic affairs in emergencies. Emergency Banking Relief Act, Pub. L. 73-1, 48 Stat. 1 (1933); Executive Proclamation No. 2039 (1933).

Congress then changed its mind. In 1977, Congress amended the 1917 Act to apply "solely to times of war." *Wald*, 468 U.S. at 227. For peacetime, it enacted a narrower authorization in IEEPA. *Id.* at 227 n.8*; accord id.* at 248-49 (Blackmun, J., dissenting). In IEEPA, Congress granted the President the power to regulate transactions during emergencies only if the transactions were international, which meant they involved Americans *and foreigners*. *See Wald*, 468 U.S. at 227 n.8 ("The grant of authorities in IEEPA does not include the power to vest (*i.e.*, to take title to) foreign assets, to regulate purely domestic transactions, to regulate gold or bullion, or to seize records.") (citing H.R. Rep. No. 95–459, pp. 14-15 (1977)); Pub. L. 95-223, 91 Stat.

1625 (1977); *see also Report of the Special Committee on the Termination of the National Emergency*, *supra*, at 5-10 (explaining this backstory and purpose). IEEPA authorized the President to restrict, in a declared emergency, transactions involving "any property in which any foreign country or a national thereof has any interest." 50 U.S.C. §1702(a)(1)(B). As the House Report explained, IEEPA eliminated the President's "power to regulate purely domestic transactions." H.R. Rep. No. 95-459, at 15.

IEEPA's requirement that a regulated activity involve a foreigner's property interest is a real limit. A "property interest" is not a vast and unknowable concept, but a familiar legal term. It is a type of "legal interest," defined as "all or part of a legal or equitable claim to or right in property." *Interest*, Black's Law Dictionary (11th ed. 2019). The existence of a "property interest" depends on whether the person has "[a]n interest ... held by an owner, beneficiary, or remainderman in land, real estate, business, or other tangible items." *Property Interest*, Black's Law Dictionary (11th ed. 2019). To be a property interest, the interest must be in "objects or rights which are susceptible of ownership," such as money or goods. *Meyer v. United States*, 364 U.S. 410, 412 n.3 (1960). The term is synonymous with "ownership interest." *See Property Interest*, Black's Law Dictionary (11th ed. 2019) ("also termed ... ownership interest"); *Ownership Interest*, Black's Law Dictionary (11th ed. 2019) ("see property interest"). When someone has a property interest in something, he typically has the "rights of possession and control," *Property Interest*, Black's Law Dictionary (11th ed. 2019), the "right to exclude," *Cedar*

Point Nursery v. Hassid, 141 S. Ct. 2063, 2072 (2021), and the right of disposition, *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982).

The Supreme Court has enforced IEEPA's property-interest requirement literally. In *Dames & Moore*, the Court considered whether IEEPA authorized the President to regulate lawsuits by Americans against the Iranian government. 453 U.S. at 675. Although the Iranian government was obviously foreign, the lawsuit itself did not involve foreign property—only a request for damages that would be paid out of foreign property—so the Supreme Court held that the President could not regulate it under IEEPA's second clause. *Id.* Lawsuits against foreigners "are not in themselves transactions involving [foreign] property." *Id.* An "in personam lawsuit, although it might eventually be reduced to judgment and that judgment might be executed upon, is an effort to establish liability and fix damages." *Id.* It "does not focus on any particular property within the jurisdiction" of the foreigner. *Id.* Because the government could not identify particular foreign property in the regulated lawsuit, it could not regulate that lawsuit within "[t]he terms of the IEEPA." *Id.*; *accord Ministry of Defense of Iran v. Elahi*, 556 U.S. 366, 376-77 (2009) (holding that foreigners lacked property interest in damages judgment in their favor until formal confirmation of arbitration award).

In short: IEEPA's requirement that any regulated transaction must include foreigners' property interests means what it says.

II. OFAC banned Americans' domestic transactions.

A. OFAC banned domestic uses of a cryptocurrency software tool.

1. Understanding what OFAC did requires a brief orientation to cryptocurrency and Ethereum. Cryptocurrency is a digital system of money. One popular online network for using cryptocurrency and similar digital assets is called Ethereum. To use cryptocurrency on Ethereum, a user generates a unique pseudonymous "address," which is a string of letters and numbers. ROA.146. She can then send or receive cryptocurrency from and to her address. *Id.*

When a user sends or receives cryptocurrency on Ethereum, the transaction is posted to a public ledger visible to anyone. ROA.918. The public ledger displays information including the sender's address, the recipient's address, and the cryptocurrency that they exchanged. ROA.924. But because the addresses are pseudonymous, only the user typically knows that the transaction is his or hers. Onlookers can identify transaction participants only if they can match a public key to an identifiable person. *See* Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 6 (2009), perma.cc/5MZP-PAEX. Once that happens, the public-ledger system actually becomes a tool for surveillance. *See id.* ("if the owner of a key is revealed, linking [on the public ledger] could reveal other transactions that belonged to the same owner"); *see, e.g., Matter of Search of Multiple Email Accts.*, 585 F. Supp. 3d 1, 8 (D.D.C. 2022) (detailing such surveillance).

Ethereum hosts multiple digital assets, but units of its native cryptocurrency are called ether or "ETH." If two friends, Bob and Alice, want to make a transaction using ETH, they can do so by having one send a unit of ETH to the other's address without going through a middleman like a credit-card company or a bank. Their transaction will look like this:

Bob's address –0.1 ETH→ Alice's address

The public ledger will display only each user's pseudonymous address and will not identify that Bob's address belongs to Bob unless he has proactively chosen to publicly associate himself with his address. But the ledger makes it possible for anyone to see all transactions associated with Bob's address for all time simply by using a publicly-available blockchain explorer, like etherscan.io.

More advanced Ethereum users also create software tools that are published to or associated with Ethereum addresses. ROA.1080. These software tools consist of computer code that performs some action when users interact with them. Typically, when someone publishes software in the form of code on the Ethereum network, the software will be permanently accessible and cannot be changed. ROA.1081. This is what it means for blockchain technology to be "immutable."

For example, a software tool could allow users to send the tool cryptocurrency, and then the software tool holds it until the value of that cryptocurrency reaches a certain price. If Bob wanted to hold his cryptocurrency until it reached that price, he could send a unit of ETH to the address that hosts this software tool.

Bob's address –0.1 ETH→ hold address

The software's code would then automatically send it back to Bob according to its rules when the price was reached.

hold address –0.1 ETH→ Bob's address

Thousands of software tools published to Ethereum addresses allow people to engage in a wide range of sophisticated transactions according to predetermined rules.

2. This case involves one such software tool. Here, OFAC banned sending or receiving anything from 91 Ethereum addresses. Those 91 addresses are identified and listed on OFAC's website and in the administrative record. *See* ROA.919-22; *Burma-related Designations; North Korea Designations; Cyber-related Designation; Cyber-related Designation Removal; Publication of Cyber-related Frequently Asked Questions*, OFAC (Nov. 8, 2022), perma.cc/98MV-HJGT; *see also Notice of OFAC Sanctions Action*, 87 Fed. Reg. 68578, 68578-68579 (2022) (listing the 91 addresses).

Of those 91 banned addresses, at least 20 take center stage. Those addresses each host essentially the same software tool, long referred to as "Tornado Cash." But in this litigation, the government and the district court lumped together people and organizations into one amorphous term, "Tornado Cash." In doing so, they inaccurately grouped together distinct entities, software tools, and persons. For clarity, DEF will call the tool at these addresses the "core software tool." The addresses that host the core software tool are listed as numbers I-XIX and LXXXVI in the administrative record. *See* ROA.919-22.

The core software tool performs a simple function. It allows users to send a cryptocurrency asset from one of their addresses and then withdraw that same asset to another one of their addresses. ROA.1083; *see also* ROA. 952 (core software tool accepts cryptocurrency units "from one address and enables their withdrawal from a different address"). The core software tool is popular because it completes this simple function in a way that solves the problem of tracing transactions on the public ledger. Users can send their cryptocurrency assets to the core software tool address, and then withdraw those assets back to themselves at another address that third-party observers cannot easily tell is theirs. ROA.955. But economically, the user simply sends and then receives his own assets. The core software tool "simply execute[s] 'deposit' and 'withdrawal' operations" that the user has decided upon and actioned. ROA.954. Nobody controls the software tool and nobody can change it. ROA.1087-89.

All 20 addresses host the same core software tool, except that each one is for sending and receiving a different amount of cryptocurrency. One address is for sending and receiving 0.1 ETH. *See* ROA.920 (address I). Another is for sending and receiving 1 ETH, another is for sending and receiving 10 ETH, and some are for other assets like "USDC" and "DAI." *See* ROA.920-22. As for the other 71 addresses, they host related software, like an optional donation tool.

An American using the core software tool therefore can just send her cryptocurrency to the address corresponding to it, like the "0.1 ETH" address, and

then withdraw the cryptocurrency to a new address at a later time. Here is what it looks like for Bob to use the 0.1 ETH version of the core software tool:

(1) Bob's address –0.1 ETH→ 0.1 ETH address (address I)

(2) 0.1 ETH address (address I) –0.1 ETH→ Bob's second address

Bob can wait any amount of time between the two steps.

This transaction is solitary because in the course of using the core software tool, a user like Bob does not have to make a payment to anyone else or transfer funds to anyone else.[2] ROA.1087-89; *see also* Gruenstein et al., *Secret Notes And Anonymous Coins: Examining FinCEN's 2019 Guidance On Money Transmitters In The Context Of The Tornado Cash Indictment*, Int'l Academy of Financial Crimes Litigators (Sept. 2023), perma.cc/V99B-NVCZ. Nobody besides Bob has any control over the asset when it resides at the core software tool address. *Id.*

If Bob is an American, then the above transaction obviously does not fall within IEEPA's second clause. It does not involve *anybody else's* property interest, let alone any "particular property" belonging to a foreigner. *Dames & Moore*, 453 U.S. at 675. The transaction involves only Bob's cryptocurrency, which everyone agrees is his own property.

[2] Everyone agrees the standard Ethereum fee that applies to all transactions does not have any legal significance here.

But all agree that OFAC's designations banned the above transaction for every American. *See FAQ: Can U.S. Persons Engage in Transactions Involving Identified Tornado Cash Virtual Currency Wallet Addresses Absent a Specific License from OFAC?*, OFAC (Nov. 8, 2022), perma.cc/PQ96-ANZS (illegal to "engage in transactions involving identified … addresses," including all 20 core software tool addresses). Although the district court focused on other possible kinds of transactions, like those involving "relayers," it ignored domestic transactions like these. But it is a federal felony today for Bob to unilaterally send his own cryptocurrency to the core software tool without relayers. *See id.*; 50 U.S.C. §1705(c) (imposing criminal penalties for transactions in violation of this order). Because OFAC's designations banned transactions like the one above—and tens of thousands a year like it, ROA.940-58—it exceeded IEEPA's second clause.

OFAC *could* have crafted more specific designations. It could have banned Americans from using the software tool to send their cryptocurrency assets to foreigners. It could have banned them from using relayers who pay money to foreigners. And it could have banned any other transactions with foreigners. But it could not prohibit all uses of the software tool, including those that do not involve any foreigners' property interests at all.

B. The district court's attempts to connect OFAC's action to foreigners' property interests are unpersuasive.

In order to avoid the straightforward conclusion that OFAC's designations banned domestic transactions, the district court drew elaborate and hypothetical

connections to foreigners. But none justify banning Americans' domestic use of the core software tool.

Relayers. The district court homed in on an optional service related to the core software tool performed by what are called "relayers." Before the ban, relayers offered a convenient service. Someone who did not want to pay to withdraw his cryptocurrency to his second address, lest it create a trail back to his first address, could pay a relayer to do it for him. ROA.1092.

But, as discussed above, relayers are not necessary to use the core software tool. Although the core software tool has been running since 2019, "the launch of the relayers" was not until "March 2, 2022." ROA.940. Even before the designations, over 16% of transactions did not use registered relayers. ROA.958. OFAC's own record documents tens of thousands of transactions that used the core software tool without relayers. ROA.940, 958.

Besides, the relayers themselves were often Americans. And for many of the 20 addresses, including the 0.1 ETH address, the relayer kept his entire relayer fee. ROA.960-61. But for *some* of the 20 addresses, a tiny payment went to a registry associated with a decentralized autonomous organization, or "DAO." ROA.957-58. And OFAC takes the position that the DAO is a "foreign" person.[3]

[3] Plaintiffs separately and persuasively dispute that position. *See* Appellants' Br. 26-34.

In the district court's view, this series of contingencies that sometimes connects to a purportedly foreign DAO justified the *entire ban* under IEEPA. The district court said that because *some* uses of *some* addresses that host the core software tool "generate fees … for the [foreign] DAO" through some of these "relayer-facilitated transactions," OFAC can prohibit *all* uses of *all* addresses that host the core software tool, regardless of whether they involve such fees. ROA.1510. By that logic, Bob's transaction diagrammed above falls within IEEPA because it could have been different, and if it were different, it would have fallen within IEEPA.

The district court cited no cases for the strange proposition that a federal agency can ban a transaction because different transactions fall within the agency's statutory authority. Of course, it cannot. *See, e.g.*, *FEC v. Ted Cruz for Senate*, 142 S. Ct. 1638, 1649 (2022) ("An agency, after all, 'literally has no power to act'—including under its regulations—unless and until Congress authorizes it to do so by statute."). When a statute authorizes an agency to ban certain transactions, it can ban only those transactions. Regardless of whether OFAC has authority under IEEPA to ban Americans from paying cryptocurrency to the DAO, it cannot ban them from engaging in wholly domestic transactions.

The district court's reasoning, if accepted, would allow OFAC to criminalize practically any domestic activity. If OFAC sought to ban an American from driving his car from his house to his country cabin, all it would have to do is allege that he *could* buy gas along the way, and that *some* gas stations pay a portion of their revenue to foreign

oil companies. Even if he drives an electric car that never generates a payment to a foreign oil company—like Bob and many other Americans who use the 0.1 ETH address and never generate a payment to the DAO—OFAC can regulate him based on *different* cars that *other* people drive. But OFAC cannot do that and should lose a challenge brought by the domestic electric car driver. While IEEPA was written to keep OFAC out of the domestic economy, the district court's reasoning would make OFAC our new economic czar. *But see Wald*, 468 U.S. at 227 n.8; *Report of the Special Committee on the Termination of the National Emergency*, *supra*, at 5-10.

Nor was banning the core software tool necessary as some sort of prophylactic. If OFAC wanted to ban all payments to the DAO, it could have done so without touching the core software tool. All payments to the DAO must go through the DAO's address. ROA.919, 960-61. OFAC did ban all transactions with that address. ROA.921 (address LXV). By doing so, it banned payments to the DAO. If OFAC had stopped there, it would have stopped all transactions with designated foreigners—and law-abiding cryptocurrency users in this country would have no complaint. But it went further and banned all uses of the at least 20 addresses that host the core software tool, even when they do not involve a payment to the DAO. *See* ROA.919-22 (I-XIX and LXXXVI). The only effect of going further was to ban domestic uses of the core software tool, like Bob's diagrammed above.

"Contracts." The district court alternatively imagined that an American's solitary use of the core software tool, like Bob's above, is actually a legal "contract."

Specifically, it imagined that it is a contract with the purportedly foreign DAO or the foreigners who first wrote the software, which it said would give foreigners a property interest in that use. ROA.1509. The primary basis for the district court's "contracts" theory was that, in the cryptocurrency world, people refer to software published on networks like Ethereum as "smart contracts." The district court asserted that "smart contracts are merely a code-enabled species of unilateral contracts," which are a valid kind of legal contract, and therefore might give rise to property interests. *Id.*

But there are no legal contracts giving rise to foreigners' property interests in an American's use of the core software tool. The term "smart contract" is a metaphor. It just means software that is designed to function according to prearranged terms, not a literal legal contract. "[T]he term 'smart contract' is a misnomer because, in many cases, a smart contract is neither smart nor a contract." *Smart Contracts and Distributed Ledger: A Legal Perspective*, ISDA 5 (2017), perma.cc/XJ2D-C4NY. Smart contracts do not require "parties." Even the district court recognized elsewhere that a smart contract is just any "tool that carries out a particular, predetermined task," without any legal requirements. ROA.1509-10. The court should not have allowed colloquialisms to dictate its legal analysis. Courts should "not rely on the labels, but rather the substance of the transactions." *Sterling Property Man. v. Tex. Commerce Bank*, 32 F.3d 964, 968 (5th Cir. 1994).

Labels aside, the core software tool does not create a "unilateral contract" or any other sort of legal contract giving rise to foreigners' property interests. A contract does not exist without "two or more parties" making an "agreement" based on "sufficient consideration" that "creat[es] obligations" on both parties. 17A Am.Jur.2d Contracts §1. A "unilateral" contract is just a subspecies of contract that is accepted by performance rather than acceptance, but it still must satisfy all these requirements. *Restatement (2d) of Contracts* §45 (1981). These elements are not met here. Nobody promised anyone anything. The software tool is free. And no one has any continuing obligation to anyone else. When Bob uses the core software tool, he does not make an agreement with any counterparty at all.

Deference. The district court still could not bring itself to conclude that OFAC's action fell within the "ordinary meaning" of the statute. ROA.1507. Instead, it ruled for OFAC by giving it multiple levels of compounding deference with no basis in modern law.

First, it gave OFAC an "even greater degree of deference than the *Chevron* standard" in defining IEEPA's requirement of a "property interest." ROA.1505. But not even *Chevron*, let alone the district court's *Chevron*-on-steroids, applies here. "Where a statute's language carries a plain meaning, the duty of an administrative agency is to follow its commands as written." *SAS Inst. v. Iancu*, 138 S.Ct. 1348, 1355 (2018). The district court acknowledged that IEEPA's "property interest" language *does* carry an

"ordinary meaning"—namely, a "legal or equitable claim to or right in property"—but then let OFAC change that meaning anyway. ROA.1507.

And regardless of whether "property interest" carries a plain meaning, *Chevron* does not apply here because OFAC is interpreting a statute that "imposes criminal penalties." *Cargill v. Garland*, 57 F.4th at 466. Courts "must not apply *Chevron* where, as here, the Government seeks to define the scope of activities that subject the public to criminal penalties." *Id.* at 467. The Supreme Court has "never held that the Government's reading of a criminal statute is entitled to any deference." *United States v. Apel*, 571 U.S. 359, 369 (2014). Here, OFAC's interpretation defines the scope of activities that subject people to 20-year prison sentences under IEEPA. 50 U.S.C. §1705(c). Under this Court's en banc precedent, the district court therefore erred in giving OFAC *Chevron* deference. *Cargill*, 57 F.4th at 467.

In fact, the district court was supposed to do the opposite. All ambiguities in IEEPA must be interpreted *against* OFAC under the rule of lenity. "The rule of lenity is a 'time-honored interpretive guideline.'" *Cargill*, 57 F.4th at 471. This Court has "applied it many times to construe ambiguous statutes against imposing criminal liability," including in challenges to agency interpretations of those statutes. *Id.* Lenity is especially important in challenges to agency interpretations of statutes because it "preserves the separation of powers 'by maintaining the legislature as the creator of crimes.'" *Id.* at 470. When a statute has both criminal and noncriminal applications, courts "must interpret the statute consistently" in both contexts. *Leocal v. Ashcroft*, 543

U.S. 1, 11 n.8 (2004). Whether the Court encounters it "in a criminal or noncriminal context, the rule of lenity applies." *Id.*; *see also United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 517-18 (1992) (plurality op.) (applying the rule of lenity to a tax statute, in a civil setting, because the statute had criminal applications and had to be interpreted consistently across its applications); *id.* at 519, 523 (Scalia, J., concurring) (same). The district court offered no reason why the rule of lenity did not apply here.

The district court then went further. It deferred to OFAC's in-litigation interpretation of its own "regulatory definitions" to which it had already given improper deference, including OFAC's interpretation of the word "contract" in its own regulation—the regulation at issue in this litigation. ROA.1509. The district court held that OFAC's interpretation of its own regulation was entitled to deference unless "plainly inconsistent" with its own regulation. *Id.* That approach violates *Kisor v. Wilkie*, 139 S. Ct. 2400, which the district court never acknowledged. Under *Kisor*, courts cannot defer to interpretations of regulations "requiring the elucidation of a simple common-law property term." *Id.* at 2417. It's hard to think of a more "simple common-law property term" than "contract." Also under *Kisor*, courts cannot defer to interpretations of regulations that reflect a "litigation position," rather than "fair and considered judgment" *Id.* at 2417-18. OFAC's position that its regulatory term "contract" encompasses the relationship here is not formalized in any preexisting agency documents and is purely a litigation position. And finally, under *Kisor*, a court cannot defer to interpretations of regulations unless it finds that the regulations are "genuinely

ambiguous." *Id.* at 2414. But the district court instead focused on whether OFAC's interpretation was "plainly inconsistent" with its own regulation. ROA.1509.

III. Americans used the cryptocurrency software tool for important and innocent reasons.

Americans value the core software tool because it solves an important problem. Again, unlike traditional financial transactions, Ethereum transactions are posted on a public ledger that anyone in the world can view. If someone can link a person's real-world identity to his Ethereum address, "it becomes possible to *trace that user's complete financial history*." ROA.1082 (emphasis added). For example, if Bob's employer makes a payment to Bob, the employer will know which address belongs to Bob and can then go review the public ledger to see all the other transactions he has made from the same address. The employer can therefore see that Bob's a millionaire, that Bob donates to a certain religious denomination, or that Bob is seeing a counselor. For obvious reasons, people don't like having all their transactions easily traceable on the public ledger.

The core software tool solves that problem. It allows Americans to cut off the traceability of their past and future transactions, so others cannot survey them all with ease. ROA.1082. Because many people are sending the same unit of cryptocurrency to the same addresses, it is impossible to tell who is withdrawing to which address when the withdrawal transactions are published. *Id.* A third party can no longer bring up a full transaction history with ease.

Responsible Americans therefore use the core software tool, in transactions like Bob's above, for many reasons. For one, it protects them from violence. Thieves can

identify cryptocurrency users with large holdings and threaten them unless they send them their assets. Popper, *Bitcoin Thieves Threaten Real Violence for Virtual Currencies*, N.Y. Times (Feb. 18, 2018), perma.cc/3KCU-3ELC. And dangerous groups, like Russians who follow donations of cryptocurrency to Ukraine, for example, can use public cryptocurrency transactions as a basis for retaliation. *Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, CISA (May 9, 2022), perma.cc/C5TN-QL62.

Americans also used the core software tool because they value privacy for the same reason that all of us value privacy. They "want to give to a political cause or religious entity without fear that they will be persecuted for their views." Tuminelli & Whitehouse-Levine, *When Did Privacy Become a Bad Word?*, CoinDesk (Aug. 25, 2023), perma.cc/26PB-ZREX. They "want to purchase items without anyone knowing to protect secrets or out of embarrassment or any other reason." *Id.* And they "want to speak freely to their friends without fear their words may be later taken out of context by a government official." *Id.*

And Americans used the core software tool because they know that governments surveil cryptocurrency transactions. *E.g., Matter of Search of Multiple Email Accts.*, 585 F. Supp. 3d at 8 (detailing government public-ledger surveillance); U.S.-Br., *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020) (same). This sort of government surveillance is "Orwellian" and wrong. *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir. 1987). The core software tool alleviates it.

The Plaintiffs in this case illustrate this point. They planned to use the core software tool to make their regular cryptocurrency activities more private, to protect their families, to keep malicious actors from detecting valuable assets, and to avoid retaliation for political donations by Russian state-sponsored hacking groups. ROA.1496-99. They are like many other Americans who used the software tool for responsible reasons and with no foreign involvement, but who would now commit a felony if they did so in the future. "Privacy of personal matters is an interest in and of itself." *Roberts v. Austin*, 632 F.2d 1202, 1214 (5th Cir. 1981). The core software tool promotes that privacy for many law-abiding Americans, and IEEPA gives OFAC no authority to criminalize their domestic transactions.

* * *

OFAC took an impermissibly broad view of its authority here. Affirming the district court's decision, which would allow it to ban domestic transactions simply because they might be modified to include foreigners, would authorize OFAC to engage in widespread regulation of domestic activities in the future. Importantly, vacatur will allow OFAC to go back to the drawing board to enact a more targeted designation that bans transactions involving foreigners while respecting IEEPA's limits.

CONCLUSION

This Court should reverse.

Dated: November 20, 2023

Respectfully Submitted,

J. Abraham Sutherland
106 Connally Street
Black Mountain, NC 28711
(805) 689-4577

/s/ Cameron T. Norris
Cameron T. Norris
Jeffrey S. Hetzel
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Ste. 700
Arlington, VA 22209
(703) 243-9423
cam@consovoymccarthy.com

Counsel for Amicus Curiae DeFi Education Fund

CERTIFICATE OF COMPLIANCE

This brief complies with Fed. R. App. P. 32(a)(7)(B) and Circuit Rule 32(c) because it contains 5,932 words, excluding the parts that can be excluded. This brief also complies with Fed. R. App. P. 32(a)(5)-(6) and Circuit Rule 32(b) because it has been prepared in a proportionally spaced face using Microsoft Word 2016 in 14-point Garamond font.

Dated: November 20, 2023 */s/Cameron T. Norris*

CERTIFICATE OF SERVICE

I e-filed this brief with the Court, which will email everyone requiring notice.

Dated: November 20, 2023 */s/Cameron T. Norris*