EXHIBIT A

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION

COIN CENTER et al., *Plaintiffs,* v. JANET YELLEN et al., *Defendants.*	Civil Action No. 3:22-cv-20375-TKW-ZCB

BRIEF OF ANDREESSEN HOROWITZ AS AMICUS CURIAE IN SUPPORT OF PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Civil Procedure 7.1, and to enable Judges and Magistrate Judges of the Court to evaluate possible disqualification or recusal, Amicus curiae AH Capital Management, L.L.C., by and through its undersigned counsel, hereby certifies that no publicly-held company owns 10% or more of AH Capital Management, L.L.C.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

Statutes

Rules and Regulations

Other Authorities

Gary Weinstein, *AI And Blockchain Analytics: The Urgent Need For Crypto Privacy Tools*, Forbes (Apr. 7, 2023), https://rb.gy/1si0l..7

I. INTEREST OF AMICUS CURIAE

Amicus curiae Andreessen Horowitz ("a16z") is a venture capital firm that invests in start-up to late-stage technology companies across a range of sectors, including the blockchain ecosystem.[1] This ecosystem has grown rapidly since it was first developed in 2008. To date, amicus's dedicated funds have raised more than $7.6 billion to invest in companies within this ecosystem. Amicus has been at the forefront of advancing the industry through investments in companies that build blockchain-based solutions relating to identity management, enterprise management, content creation, environmental protection, data storage, and many other sectors. Amicus has significant expertise relating to the unique attributes of crypto assets and decentralized systems and employs a dedicated team of engineers and scholars in these fields.

Amicus's long-standing participation in the blockchain ecosystem supports its strong interest in the law relating to blockchains. For the first time, decentralized blockchain-based protocols allow everyday users and creators greater access, ownership, and control of their data, activities, and actions on the Internet, rather than having to rely on centralized protocols that give this power to large, third-party corporate entities. That newfound freedom is now threatened, as the Office of Foreign Assets Control ("OFAC") has applied its powerful sanctions authority to effectively disable decentralized, open-source, and ownerless software that was used by thousands of users to add a layer of privacy to their crypto asset transactions on the blockchain. Amicus has a particularly strong interest in this case because decentralized software is a foundational technology in the development of the Internet.

OFAC's decision to sanction Tornado Cash raises serious, far-reaching legal questions that not only affect our portfolio companies, but also the blockchain ecosystem far beyond this case,

[1] A more fulsome explanation of blockchains appears in Section III.A, *infra*.

including companies that develop decentralized protocols and the applications that developers build on top of them. For this reason, amicus respectfully offers this brief to assist the Court in understanding decentralized software and the significant statutory deficiencies inherent in OFAC's application of sanctions against Tornado Cash.

II. INTRODUCTION AND SUMMARY OF ARGUMENT

This case presents a complex question at the intersection of emerging technologies and the government's power to impose economic sanctions. OFAC's use of its sanctions authority against the Tornado Cash software is the first time that open-source, decentralized, and ownerless software code has been the target of U.S. sanctions. To justify this novel application of sanctions, OFAC relies on two statutes: (1) the International Emergency Economic Powers Act, which empowers the Executive Branch to deal with national emergencies by blocking "transactions involving[] any property in which any foreign country or a national thereof has any interest," 50 U.S.C. § 1702(a)(1)(B), and (2) the North Korea Sanctions and Policy Enhancement Act, which provides supplemental authority for blocking "all transactions in *property* and *interests in property* of a person designated" for engaging in certain activities involving North Korea. 22 U.S.C. § 9214(c)(1) (emphases added); *see also* 22 U.S.C. § 9214(c)(2); 31 C.F.R. § 578.802 (OFAC's Cyber-Related Sanctions Regulations); 31 C.F.R. § 510.802 (North Korea Sanctions Regulations). OFAC sanctioned Tornado Cash[2] pursuant to these statutes.

These statutes do not authorize the sanctioning of open-source, decentralized software that no one owns. While amicus understands and supports the government's desire to neutralize North Korea's ability to launder the proceeds of illicit activity that support weapons proliferation activities, it cannot do so by exceeding its statutory authority. In this instance, OFAC has

[2] The exact targets of OFAC's sanctions are the "tornado.cash" website and specific "digital currency addresses" available at https://rb.gy/jrwc7.

overstepped its statutory authority in violation of the Administrative Procedure Act ("APA") in at least two ways.

First, OFAC lacks congressional authorization to sanction the ownerless Tornado Cash smart contracts (the "Smart Contracts")[3] based on their statutory authority to regulate "property." At the time it designated Tornado Cash, OFAC published certain "identifiers" associated with Tornado Cash, including dozens of blockchain addresses.[4] The implication of the OFAC designation is that the Smart Contracts are property and, as a result, are blocked and sanctioned. However, the Smart Contracts, as described below, lack any of the long-recognized attributes of property. For centuries, common law principles have guided our understanding of the meaning of "property." Specifically, in order for something to be property, one or more people must be able to possess, exclude others from, control, dispose of, or enjoy that thing. But the Smart Contracts are simply lines of open-source, computer code that no person can possess, alter, or control. No one can exclude another person from using, altering, or removing the Smart Contracts, and no one will *ever* be able to control, alter, or remove the Smart Contracts. If OFAC can sanction these Smart Contracts, then its power to sanction has no limits with respect to software.

Second, and similarly, OFAC lacks Congressional authorization to prohibit interactions with those ownerless and immutable Smart Contracts based on its authority to regulate transactions involving "interests in property." No person or entity has an "interest" — i.e., a legal or beneficial claim — in the Smart Contracts. Rather, the Smart Contracts are self-executing software programs that are accessible for everyone to use. As with the first argument, OFAC's unilateral expansion

[3] The defined term "Smart Contracts," as discussed herein, refers ***only to the 29 sanctioned addresses*** that Plaintiffs challenge in the First Amended Complaint ("FAC"). A full list of these addresses can be found in the FAC's Appendix on Pg. 41 (ECF No. 9). *See also* Plaintiffs' discussion at Pg. 6-8 of the Motion for Summary Judgment (ECF No. 36).

[4] OFAC, *Burma Related Designation; Cyber-related Designation; Cyber-related Designation Removal; Publication of Cyber-related Frequently Asked Questions* (Nov. 8, 2022), https://ofac.treasury.gov/recent-actions/20221108.

of its sanctioning authority lacks a limiting principle and thus constitutes unprecedented Executive Branch overreach.

In sum, OFAC exceeded its statutory authority and violated the APA when it sanctioned decentralized, self-executing, open-source, and ownerless software. The thousands of users impacted by OFAC's sanctions are depending upon the Court to use its power to invalidate the challenged actions. It is the sole prerogative of the Legislature to expand OFAC's authority, and it has not done so. For these reasons, this Court should grant the Plaintiffs' motion for summary judgment.

III. **BACKGROUND**

Most important Internet applications could not exist without significant privacy protections for their users. Email, messaging, and banking applications, for example, depend on the confidential exchange of sensitive information and data. Few users would accept otherwise. If online banking applications exposed the contents of users' bank accounts to the world, the security of an untold number of users would be jeopardized, leaving future users reluctant to use online banking services. But transparency is currently the standard practice of most blockchain networks, such as Ethereum — the blockchain that underlies most Tornado Cash smart contracts.

A. The Contours of the Underlying Technology Are Crucial to the Court's Decision.

As a threshold matter, a blockchain is simply a network of computers on the Internet. Blockchains are also commonly referred to as "public ledgers" because much of the data, though not all, on these "ledgers" relates to financial transactions.[5] Ethereum uses blockchains and peer-to-peer networking to generate a shared world computing platform that can flexibly and securely

[5] *See Blockchain Technology Explained in Simple Terms*, WorldCoin, https://rb.gy/43w8d (last visited June 1, 2023).

run any software application users want to code.[6] The Ethereum blockchain works in a distributed manner to create a public database of information, which includes financial transactions. Each transaction completed on the Ethereum blockchain is recorded and posted on its database, or transparent public ledger, which anyone can view on a computer. *See* Am. Compl. ¶ 43. This aspect of the Ethereum blockchain is similar to a bank's ledger used to record customer information, but with a critical difference. Traditional bank ledgers, for example, are centralized, private, and modifiable. Most blockchains, on the other hand, are decentralized, public, and unchangeable. The default of the Ethereum blockchain, for instance, is transparency, and every transaction that occurs on it is publicly viewable and irreversible. As a result, an Ethereum blockchain address's entire transaction history on that network is viewable to anyone with access to an Ethereum block explorer website.[7] *See* Am. Compl. ¶ 3. Because of the public nature of the Ethereum blockchain, there are several methods, described below, in which the identities of people behind transactions can be revealed, along with their cryptographic addresses, transactions, and assets.

Ethereum's network also enables developers to build applications on top of it and allows users to hold assets and transact and communicate over the network without third-party intermediaries. Ethereum is decentralized, meaning that no person, company, or institution, such as a bank or other financial services company, needs to serve as a conduit between parties that interact with one another on the network.

Ethereum provides numerous benefits to its users. Because the Ethereum blockchain does not require any third-party intermediaries, transactions can occur at any time of day or night, are generally settled faster than non-blockchain-based transactions, and are secured through the use of

[6] *See* Vitalik Buterin, *Ethereum*, Coin Center (Mar. 9, 2016), https://rb.gy/j52lb; *see also* Am. Compl. ¶¶ 2, 41.

[7] *See, e.g.*, Ethereum (ETH) Blockchain Explorer, https://etherscan.io/ (last visited June 1, 2023).

cryptography rather than through a trusted third party. The Ethereum blockchain and the smart contracts operating on it provide safe, low-cost access for people of any race, nationality, or background to conduct transactions.

B. Privacy Is Central to a Well-Functioning Internet.

Despite these benefits, the only privacy protection for most blockchain users, including Ethereum users, is the pseudonymity of users' accounts. Specifically, the "accounts" listed on the Ethereum blockchain are not associated with the actual names of Ethereum users, but rather with algorithmically generated "addresses."[8] A cryptographic address is akin to a username, email address, phone number, or bank account number, depending on its function. Ethereum users who transfer crypto assets — for instance, Ether (abbreviated as ETH), the native cryptocurrency to the Ethereum blockchain — use such a public facing address. *See, e.g.*, Am. Compl. ¶¶ 2, 45. But the pseudonymity of an Ethereum address is rarely sufficient to preserve a user's privacy and prevent a network observer from connecting a public address with a real-life identity. Once a user interacts with another person or entity, the user's entire on-chain transaction history is exposed, and potentially their identity revealed, because it can be traced back from the known public address. *Id.* ¶ 45. Indeed, there are a plethora of individuals and companies with expertise in conducting blockchain analytics to overcome crypto asset address pseudonymity.[9]

The ease with which crypto asset address pseudonymity can be overcome is a serious challenge for the future of blockchains. Despite the technological innovation blockchains present, it also creates a major paradox in privacy. Participants in blockchain networks can trust the veracity of the information on the network because they can see and verify the details themselves.

[8] An Ethereum address, for example, looks like this: 0x165CD37b4C644C2921454429E7F9358d18A45e14.

[9] Liam Glennon et al., *The Power of Analytics in the Digital Asset Economy*, Accenture (Aug. 23, 2022), https://rb.gy/hznkj.

However, that same transparency poses a real threat to an individual's privacy, not to mention the potential threat to one's safety,[10] and may chill the use of this important technology. Users are disincentivized from moving their financial data on-chain if that means exposing that data to the entire world. The same concerns apply to non-financial data as well, such as private healthcare information and other deeply personal data.

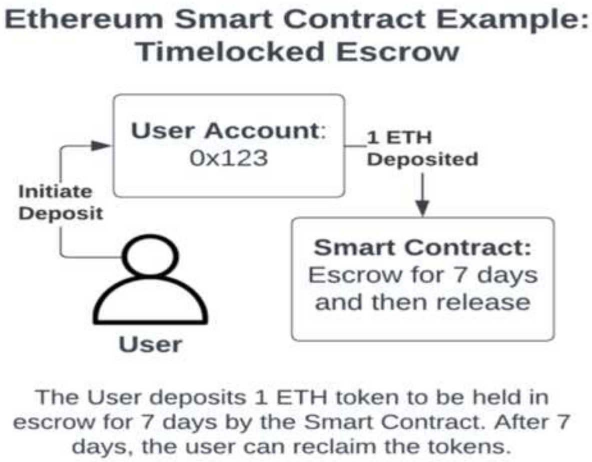
In addition to the privacy implications of having such sensitive data on-chain, there are other important risks that run the gamut in terms of severity. Take the instance of a mom-and-pop shop that accepts payment in cryptocurrency from its customers. The store's cashiers could access some of their customer's financial activity information; for example, where that customer shopped yesterday, if that activity was conducted on-chain, or the customer's total crypto holdings on the respective blockchain network used for the transaction. Larger risks also abound for individuals conducting non-private blockchain transactions, including surveillance from bad actors, consumer scams, and other potentially harmful consequences. Former Supreme Court Justice William O. Douglas was prescient in stating that "[t]he right to be let alone is indeed the beginning of all freedom," as most Internet users will always value privacy over other benefits of blockchains. *Public Utilities Comm'n of D.C. v. Pollak*, 343 U.S. 451, 467 (1952) (Douglas, J., dissenting).

C. Privacy-Preserving Technologies Like Tornado Cash Protect User Anonymity.

To combat the risk of identity and financial transaction history exposure, many users of Ethereum turn to privacy tools such as the Tornado Cash smart contracts. Privacy-preserving technologies like Tornado Cash emerged as effective solutions to the problem of protecting user anonymity. Tornado Cash smart contracts are a public, open-source software tool. All smart

[10] Gary Weinstein, *AI And Blockchain Analytics: The Urgent Need For Crypto Privacy Tools*, Forbes (Apr. 7, 2023), https://rb.gy/1si0l.

contracts are, essentially, software applications available to any member of the public on certain blockchains.[11] Am. Compl. ¶ 47. The computer code that underlies smart contracts automatically executes all or part of an operation for a user, and when developers program and configure smart contracts, they decide what operations the smart contract will support and what rules those operations must follow.[12]


Ethereum Smart Contract Example:
Timelocked Escrow
User Account:
0x123
1 ETH
Deposited
Initiate
Deposit
Smart Contract:
Escrow for 7 days
and then release
User
The User deposits 1 ETH token to be held in escrow for 7 days by the Smart Contract. After 7 days, the user can reclaim the tokens.

Source: Wade, *supra* n.11.

Certain Tornado Cash smart contracts are known as "pool" contracts; it is these pools that create the privacy-preserving function. Specifically, the smart contract pools allow users to deposit crypto assets from one address and later withdraw the same amount from a different address.[13] In so doing, the smart contracts use zero-knowledge proofs that verify the transaction without leaking specific details of the transaction. A zero-knowledge proof is a cryptographic method whereby "one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier." A.R. 34 n. 41; *see also*

[11] *See Introduction to Smart Contracts*, Ethereum (Sept. 1, 2022), https://rb.gy/eaadm; Alex Wade et al., *How does Tornado Cash work?*, Coin Center (Aug. 25, 2022), https://rb.gy/ht0d3.

[12] *See* Stuart D. Levi & Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, Harvard Law School Forum on Corporate Governance (May 26, 2018), https://rb.gy/ycpl9.

[13] *Id.*

A.R. 553. Although these transactions are publicly viewable on Ethereum's blockchain, they are not linked to the user, which ensures the user's privacy and shields the user's financial history from prying eyes.

Importantly, the Smart Contracts are completely autonomous. In other words, no individual owns them, and there is no operator. While the code that comprised the initial Tornado Cash software gave its developers certain control over prior versions of the smart contracts, the goal of the developers at the time was to transition certain of the smart contracts to full decentralization that would allow them to function without an operator, which they achieved in May 2020.[14] Because the Smart Contracts were part of this transition, transactions occur through them autonomously via self-executing code and without the assistance of intermediaries. *See* Am. Compl. ¶ 48. The code for core Tornado Cash smart contracts (i.e., the Tornado Cash pools) is viewable on GitHub,[15] a free, publicly available website popular with software developers, as well as on Etherscan. Anyone with an Internet connection can view, copy, and use the code. In addition, the Smart Contracts are immutable, meaning that they cannot be altered or removed. *See* A.R. 2146. Finally, the Smart Contracts are non-custodial, meaning that Tornado Cash users retain ownership and control of the crypto assets they send to the Smart Contracts, so neither the Smart Contracts nor anyone else other than the user takes custody of the funds. *See* A.R. 551; Am. Compl. ¶ 50.

D. Financial Privacy Is an Important Human Interest.

Privacy is a central tenet behind the development of crypto assets and blockchains. The ability to transact without fear of public exposure is an interest held dear amongst populations

[14] Tornado Cash, *Tornado.cash version 2 has been released*, Medium (Dec. 17, 2019), https://rb.gy/bkrrf; William Foxley, *Developers of Ethereum Privacy Tool Tornado Cash Smash Their Keys*, CoinDesk (May 18, 2020, updated Sept. 14, 2021), https://rb.gy/o5x6f.

[15] *Tornado Cash*, GitHub, https://github.com/tornadocash (last visited June 1, 2023).

across the globe. Individuals who live in authoritarian regimes, for example, find value, safety, and protection in private transactions. Because their lives are more subject to government surveillance, control, and oversight than non-authoritarian regimes, individuals who undertake public transactions in these countries are subject to real risks of harm. Individuals living within the United States similarly hold strong interests in the right to financial privacy.[16] Private financial transactions, for instance, offer U.S. citizens a means to exercise other rights that are fundamental to them, such as individuals seeking to pay for sensitive and highly personal healthcare, or individuals attempting to raise money for political causes important to them but socially unpopular. Reducing or eliminating financial privacy hinders the ability of individuals to protect other rights granted to them.

Before the modern-day proliferation of the Internet, financial transactions between parties enjoyed measures of privacy generally not seen today. For example, cash transactions conducted outside of financial intermediaries such as banks and other reporting-obliged entities offer such privacy and anonymity. But as individuals move from transacting in physical cash to transacting digitally online, the same privacy protections that individuals once took for granted may no longer apply. It is, therefore, no surprise that certain segments of our society have sought to reclaim this privacy. Privacy tools like the Smart Contracts serve that fundamentally legitimate purpose: they allow users to safeguard their financial privacy when choosing to transact without traditional financial intermediaries.

This all makes sense in a world of increasing threats to privacy. For example, financial institutions can sell Americans' financial and transaction data to other companies. The selling of

[16] The importance of financial privacy is not a novel concept in the U.S. For instance, the Right to Financial Privacy Act of 1978 (RFPA) protects the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records. *See* 12 U.S.C. §§ 3401-3423.

big data has often gone unchecked and without customer redress. It is precisely software tools like Tornado Cash that provide individuals with an alternative method of protecting their data, limit third-party access to their financial transactions, place leverage back into the hands of the individual, and increase personal autonomy. Although the government has legitimate concerns about national security and preventing crime, privacy-preserving technologies keep users safe against various bad actors, such as people seeking to harass or "dox"[17] others, or criminals attempting to gain knowledge of an individual's financial footprint and holdings.

IV. ARGUMENT

A. OFAC's Sanctioning of Tornado Cash Exceeds Its Statutory Authority.

"Administrative agencies are creatures of statute. They accordingly possess only the authority that Congress has provided." *NFIB v. Dep't of Labor*, 142 S. Ct. 661, 665 (2022). Here, OFAC's application of sanctions to open-source decentralized Smart Contracts is unprecedented and a unilateral expansion of the Executive Branch's power beyond what Congress has provided.

Under Executive Orders 13722 and 13694, OFAC is authorized to sanction "persons" who have provided support to the North Korean government or engaged in certain malicious cyber activities. 80 Fed. Reg. 18,077 (Apr. 1, 2015), *amended by* 82 Fed. Reg. 1 (Dec. 28, 2016); 81 Fed. Reg. 14,943 (Mar. 15, 2016). And the Executive Orders, in turn, are based on certain statutes with clear text. First, the International Emergency Economic Powers Act ("IEEPA") provides for sanctions against "property in which any foreign country or a national thereof has any interest." 50 U.S.C. § 1702(a)(1)(B). Second, the North Korea Act ("NKA") provides for sanctions against "property and interests in property" of "a person" who knowingly engages in certain conduct. 22 U.S.C. § 9214(c). It is the sole prerogative of the Legislature to expand these terms.

[17] "Dox" means to "publicly identify or publish private information about (someone) especially as a form of punishment or revenge." *Dox*, Merriam-Webster.com Dictionary, https://rb.gy/62vv0 (last visited June 1, 2023).

As outlined below, these statutes do not contemplate the power to sanction open-source, decentralized, and ownerless software code because it is not "property" or an "interest[] in property." A holding otherwise would allow the Executive Branch to deprive the Legislature of its right to circumscribe the power to sanction and would "be contrary to the basic concept of separation of powers and the checks and balances that flow from the scheme of a tripartite government." *United States v. Nixon*, 418 U.S. 683, 704 (1974) (citing The Federalist, No. 47 at 313 (S. Mittell ed. 1938)). For this reason, the Court should grant Plaintiffs' motion for summary judgment.

i. The Tornado Cash Smart Contracts Are Not "Property"

A review of dictionaries, as well as legal and historical precedent, provides sufficient reason to reject any notion that the Smart Contracts constitute "property." "A common idiom describes property as a 'bundle of sticks'—a collection of individual rights which, in certain combinations, constitute property."[18] Known as the "strands" from the "bundle of rights" theory of property, there are several generally recognized basic attributes of property, namely the rights of (i) possession, (ii) exclusion, (iii) control, and (iv) disposition (or transfer). Unlike the notion that property is some physical thing in some person's possession, this common law view defines property relationally through a set of rights. Indeed, as one court described, the common law conception of property "denote[s] the group of rights inhering in the citizen's relation to the physical thing, as the right to possess, use and dispose of it."[19] For this reason, the common law view is most appropriate to understand, as here, whether some intangible thing — namely, a set of computer code residing on the Ethereum blockchain — can be property. As shown below, whether

[18] *United States v. Craft*, 535 U.S. 274, 278 (2002) (citing B. Cardozo, *Paradoxes of Legal Science* 129 (1928) (reprint 2000)).

[19] *United States v. Gen. Motors Corp.*, 323 U.S. 373, 377–378 (1945); *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1003 (1984).

considered independently or collectively, the Smart Contracts feature none of the characteristics of property. OFAC's unprecedented and unilateral decision to include software code to the Specially Designated Nationals and Blocked Persons ("SDN") List necessitates that Congress expand the categories of things to which OFAC is authorized to apply sanctions.

The Right of Possession

As Plaintiffs and other amici have noted, dictionaries have long defined "property" to include possession or ownership, terms which are often used interchangeably.[20] Samuel Johnson, for example, defined property broadly as "[r]ight of possession," "[p]ossession held in one's own right," and "[t]he thing possessed." 2 Samuel Johnson, *Dictionary of the English Language* (1755 ed.); *see also Property*, Black's Law Dictionary 1095 (5th ed. 1979) ("everything which is or may be the subject of ownership, whether a legal ownership, or whether beneficial, or a private ownership.").[21] Legal precedent is the same. Although IEEPA and NKA do not define "property," the Supreme Court has defined "property" as "all objects or rights which are susceptible of ownership." *Meyer v. United States*, 364 U.S. 410, 412 n.3 (1960). The Smart Contracts cannot be possessed. While under certain circumstances, computer code may be arguably owned or possessed, as in the case where a person retains intellectual property rights to code that he or she wrote, the Smart Contracts are, by design, freely available for public use and viewing. Since everyone has access to use the Smart Contracts at any time, no one can be said to own or possess the code.

[20] *Possession*, Merriam-Webster.com Dictionary, https://www.merriam-webster.com/dictionary/possession#:~:text=pos%C2%B7%E2%80%8Bses%C2%B7%E2%80%8Bsion,property%20without%20regard%20to%20ownership (last visited June 1, 2023).

[21] *See, e.g.*, *Property*, Oxford English Dictionary (2d ed. 1989); *Property*, Webster's New World Dictionary of the American Language (college ed. 1968); *Property*, Webster's Third New International Dictionary (1961).

The Right of Exclusion

The "right to exclude others" is "one of the most essential sticks in the bundle of rights that are commonly characterized as property." *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979). Historical sources concur. President James Madison defined property as "that dominion which one man claims and exercises over the external things of the world, in exclusion of every other individual."[22] English jurist William Blackstone famously defined property as "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe."[23] But the Smart Contracts lack this essential characteristic. The Smart Contracts are freely available on the Internet. No one can exclude anyone else from accessing and using the Smart Contracts, and therefore they carry with them no right of exclusion.

The Right of Control

Because no individual possesses a legitimate or practicable claim to exercise exclusive control over the lines of code that constitute the Smart Contracts, they are not property. Control is defined under common law principles as the ability of someone to alter something. For example, courts have found that intangible items which individuals cannot alter, such as phone numbers, do not constitute property. *See, e.g.*, *In re StarNet, Inc.*, 355 F.3d 634, 637 (7th Cir. 2004) ("No one has a property interest in a phone number."); *cf. In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1075 (N.D. Cal. 2012) ("personal information" — e.g., a user's location, zip code, and device identifier — is not property because it is not "an interest capable of precise definition" or "capable of exclusive possession or control"). Like phone numbers, the Smart Contracts cannot

[22] *Property, James Madison, Papers 14:266—68*, Univ. of Chicago Press, https://rb.gy/f493i (last visited June 1, 2023).

[23] 2 William Blackstone, Commentaries on the Laws of England 2 (Univ. of Chicago Press 1979).

be altered or controlled by anyone. They are immutable, autonomous, and self-executing open-source code that exist on a blockchain.[24]

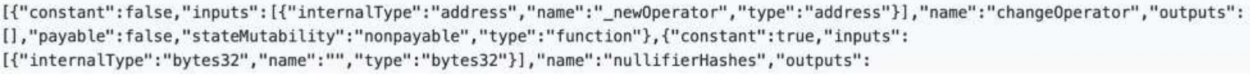
The Right to Dispose or Transfer

Likewise, the Smart Contracts also lack another fundamental characteristic of property — the right of disposal or transfer. Courts have long recognized that the right to "dispose" of or "unilaterally alienate the property" is among the rights found in the traditional bundle of property rights.[25] The Smart Contracts are publicly available, and anyone can use them at any time. If there is a thing that anyone can have without limitation at any time, it does not make sense that such a thing can be meaningfully disposed of or unilaterally transferred from one person to another.

ii. The Tornado Cash Smart Contracts Are Not "Contracts"

Smart contracts are also not property under OFAC's broad regulatory definition of property, despite the regulation's inclusion of the term "contract."[26] This argument — which is premised on the notion that the nomenclature of "smart *contract*" means that these software programs are *literal* contracts — belies the distinct functional features of the software. While the term "contracts" is not defined in IEEPA, it has long been understood under common law principles to require offer, acceptance, and consideration. Importantly, the Smart Contracts do not meet any of these requirements. In fact, smart contracts are neither "smart" nor "contracts"; the

[24] It is not possible, from a technical perspective, to alter the Smart Contracts. They have embedded code with an "_operator" variable that indicates the address of the entity that controls the contract. The current state of the operator is set to "0" for the Smart Contracts and that software code is *inalterable*:



```
[{"constant":false,"inputs":[{"internalType":"address","name":"_newOperator","type":"address"}],"name":"changeOperator","outputs":
[],"payable":false,"stateMutability":"nonpayable","type":"function"},{"constant":true,"inputs":
[{"internalType":"bytes32","name":"","type":"bytes32"}],"name":"nullifierHashes","outputs":
```

Because the software code is set to "0," no entity will ever be able to alter these smart contract addresses or otherwise exert control over them.

[25] *Craft*, 535 U.S. at 283–84; *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982).

[26] 31 C.F.R. § 515.311.

term is merely a developer-adopted and commonly used way to describe this software.[27] Instead, the Smart Contracts are computer programs that any user can access and interact with on the Internet. In the case of the Smart Contracts, anyone can use the code to transfer crypto assets from one wallet that the user controls to another wallet. Smart Contracts do not require consideration to operate as intended. Therefore, the Court should reject any purported equivalence between smart contracts and actual contracts based on generic terms alone, and recognize, as Romeo Montague did in Shakespeare's play, that "the name of a thing is chimerical, while its features are essential."[28]

iii. No One Has an "Interest" in or "Ownership" of the Smart Contracts

Critical to the government's assertion that the Smart Contracts are property is Tornado Cash's purported "interest in" or "benefit" derived from them. OFAC cannot justify its application of sanctions to Tornado Cash smart contracts broadly on the argument that a "foreign country or a national thereof" or other "person" has an "interest" in the smart contracts. Various legal definitions of the term "interest," as well as long-standing legal precedent, reveal that it is impossible for one to own an "interest" in a tool that mimics a free public good. Therefore, OFAC cannot justify its application of sanctions to the Smart Contracts on the theory that Tornado Cash has an "interest" in them. The plain language of IEEPA and the NKA set forth precisely these requirements, which OFAC failed to meet before sanctioning the Smart Contracts.

Moreover, OFAC's treatment of the term "property interest" is overbroad and impractical. The term "property interest" typically refers to a legally enforceable right to possess or use

[27] Indeed, the founder of Ethereum, Vitalik Buterin, tweeted: "To be clear, at this point I quite regret adopting the term 'smart contracts'. I should have called them something more boring and technical, perhaps something like 'persistent scripts'." Vitalik Buterin (@VitalikButerin), Twitter (Oct. 13, 2018, 1:21 pm), https://rb.gy/ml2nb.

[28] William Shakespeare, Romeo & Juliet act 2, sc. 2, in The Oxford Shakespeare: The Complete Works of William Shakespeare (W.J. Craig ed., 1914) (1597) ("What's in a name? that which we call a rose / By any other name would smell as sweet."); Jake Linford, A Linguistic Justification for Protecting "Generic" Trademarks, 17 Yale J.L. & Tech. 110, 152 (2015).

property. *See Interest*, Black's Law Dictionary (11th ed. 2019) (defining "interest" partly as "all or part of a legal or equitable claim to or right in property"); *see also In re Rogers*, 513 F.3d 212, 218 (5th Cir. 2008) (the term "'interest' refers to some legal or equitable interest that can be quantified by a monetary figure") (citing *Wallace v. Rogers (In re Rogers)*, 354 B.R. 792, 796 (N.D. Tex. 2006)). A property interest ultimately is more than "an abstract need or desire," or a "unilateral expectation," but instead must be a "*legitimate* claim of entitlement." *Bd. of Regents of State Colleges v. Roth*, 408 U.S. 564, 577 (1972) (emphasis added). An impermanent, contractual right to use an Internet domain name or phone number, for example, does not necessarily confer an interest in property. *In re Alexandria Surveys Int'l, LLC*, 500 B.R. 817, 822 (E.D. Va. 2013) ("[N]either telephone numbers nor domain names were garnishable personal property because 'neither one exists separate from its respective service that created it.'") (citing *Network Sols., Inc. v. Umbro Int'l, Inc.*, 529 S.E.2d 80, 87 (Va. 2000)), *aff'd*, 589 F. App'x 126 (4th Cir. 2014).

V. OFAC'S SANCTIONING OF THE SMART CONTRACTS LACKED LIMITING PRINCIPLES AND, IF UNCHECKED, WILL HAVE FAR-RANGING CONSEQUENCES BEYOND THE WORLD OF BLOCKCHAIN TECHNOLOGY

The arbitrary nature of OFAC's sanctioning of the Smart Contracts lacks important limiting principles. The government's position confers upon itself authority to sanction any service, software, tool, or code it might deem "property." As a practical matter, users of blockchains may now fear that the government could sanction any ownerless technical means or software that they use to effectuate transactions. The potential harms are broader reaching as well: if the government can unilaterally expand the meaning of "property" beyond its normal definition, there is a risk that it will authorize sanctions in ways that Congress did not contemplate.

For example, under OFAC's interpretation, the U.S. could sanction any open-source email protocol, e.g., SMTP, POP3, IMAP, on the basis that any email communication's content has the potential to be a conduit for illegal activity. Similar to the open-source nature of Tornado Cash smart contracts, email protocols are freely available to the public and decentralized in terms of their management; in essence, the protocol operates autonomously for anyone to use. And like the Tornado Cash smart contracts, users of email protocols do not have a "property interest" in the code because there is no legally enforceable right to use it or exclude others from using it. Under OFAC's reasoning in this case, the government could designate and block access to email protocols regardless of the fact that (i) an open-source email protocol is simply a software tool open for use in any manner to any member of the public, and (ii) the majority of users of email view it as a necessity and do not use it for unlawful or malign purposes. Allowing OFAC to wield its authority as it has in this case could yield dangerous results and would run afoul of their statutory authority. Thus, OFAC's statutory interpretation lacks a limiting principle.

VI. CONCLUSION

Our nation faces grave national security challenges, and amicus wholeheartedly supports the government in defending us from adversaries, like North Korea. Without the safety and security that the government provides, our companies could not advance technologies that benefit all Americans. Amicus, however, believes that OFAC's blanket and novel sanctioning of decentralized, open-source, and ownerless software exceeds the statutory authority that Congress has granted OFAC and is contrary to American technological and economic leadership — equally crucial pillars in ensuring our nation's security.

For the foregoing reasons, the Court should grant Plaintiffs' motion for summary judgment.

Dated: June 2, 2023

Respectfully submitted,

/s/ Alessio Evangelista
Alessio Evangelista (*lead attorney; admitted pro hac vice*)
Jessie K. Liu (*lead attorney; admitted pro hac vice*)
SKADDEN, ARPS, SLATE,
MEAGHER & FLOM LLP
1440 New York Avenue N.W.
Washington, D.C. 20005
Tel.: (202) 371-7270
Fax: (202) 661-9170
alessio.evangelista@skadden.com
jessie.liu@skadden.com

Counsel for Amicus Curiae Andreessen Horowitz

CERTIFICATE OF SERVICE

I hereby certify that on June 2, 2023, I caused the foregoing to be filed with the Clerk of Court and served upon all counsel of record via the CM/ECF system.

/s/ Alessio Evangelista
Alessio Evangelista