February 12, 2019

VIA FAX and US MAIL

Brent J. Fields, Secretary
U.S. Securities and Exchange Commission
100 F. Street, N.E.
Mail Stop 1090
Washington, D.C. 20549-1090
Fax: (202) 772-9324

Re: *In the Matter of Zachary Coburn*, *(File No. 3-18888)*

I. Introduction

The Electronic Frontier Foundation (EFF) is concerned that certain language in a recent public statement and in the SEC's Order involving the EtherDelta smart contract could be read to imply that persons engaged in merely writing and publishing computer code could run afoul of U.S. securities laws. The statement raises significant concerns for EFF because imposing liability for, or prior restraints on, publishing and distributing code would violate the First Amendment and chill innovation.

In the Matter of Zachary Coburn, the SEC initiated enforcement proceedings against the creator of EtherDelta. The action was based in part on the fact that, according to the SEC, Coburn "wrote and deployed the EtherDelta smart contract to the Ethereum Blockchain" and that he "should have known that [these actions] would contribute to EtherDelta's violations and thus, under Exchange Act Section 21C(a), caused EtherDelta to violate Section 5 of the Exchange Act." *In the Matter of Zachary Coburn*, Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order, Release No. 84553, page 9, File No. 3-18888 (November 8, 2018).

In a related public statement one week later, the SEC wrote:

> A system uses established non-discretionary methods if it provides a trading facility or sets rules. For example, an entity that provides an algorithm, run on a computer program or on a smart contract using blockchain technology, as a means to bring together or execute orders could be providing a trading facility. As another example, an entity that sets execution priorities, standardizes material terms for digital asset securities traded on the system, or requires orders to conform with predetermined protocols of a smart contract, could be setting rules. Additionally, if one entity arranges for other entities, either directly or indirectly, to provide the various functions of a trading system that

> together meet the definition of an exchange, the entity arranging the collective efforts could be considered to have established an exchange.

Statement on Digital Asset Securities Issuance and Trading, Division of Corporation Finance, Division of Investment Management, and Division of Trading and Markets, SEC.gov, https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading (November 16, 2018).

EFF respectfully submits this letter to voice its concerns that the SEC's broad language (for example, regarding "an entity that provides an algorithm" and the act of writing and deploying code) could be read to encompass anyone publishing code and working to develop systems that could benefit the public, including computer programmers and cryptographic researchers.[1] Because publishing code is speech protected by the First Amendment, such an outcome would be unconstitutional, and would undermine important policy goals such as ensuring that innovation in blockchain and distributed ledger technology can continue to flourish. EFF urges the SEC to clarify that it recognizes and upholds these vital constitutional protections.

II. About the Electronic Frontier Foundation

EFF is a non-profit civil liberties law and technology organization. Founded in 1990, EFF champions individual privacy, free expression, and innovation. With over 39,000 members worldwide, EFF uses public education campaigns, impact litigation, open source technology projects, policy analysis, and grassroots activism to ensure that civil liberties are protected in the digital age.

Central to EFF's advocacy and its history is the belief that those who write and publish software enjoy the same constitutional protections as any other speaker or publisher. That is why EFF led the legal fight more than 20 years ago to establish that the act of writing and publishing code is fully protected by the First Amendment. *Bernstein v. DOJ*, 176 F.3d 1132 (9th Cir. 1999).[2] EFF also allows supporters to make donations through Bitcoin, Ethereum, Litecoin, and Zcash.

III. Background

Blockchain technology (or distributed ledger technology) distributes a record of transactions across a network of computers. Its fundamental innovation combines

---

[1] EFF takes no position on whether other aspects of EtherDelta violated the law or SEC regulations.

[2] *See* Allison Dame-Boyle, *EFF at 25: Remembering the Case that Established Code as Speech*, EFF Deeplinks (April 16, 2015), https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech.

decentralized consensus (ensuring the majority of participants agree on the transaction history) with two important properties: censorship-resistance (allowing any entity to publish to this record) and auditability (preventing any individual from tampering with the record). In many cryptocurrency applications of blockchain technology, this allows people to securely exchange digital assets (such as cryptocurrencies) directly with each other. Because entities can easily audit and verify transactions themselves by consulting the ledger, this removes the need for an intermediary to do so. Bitcoin—the first successful implementation of blockchain technology—was envisioned as a decentralized electronic payment system that would operate independently of financial institutions.

There are many potential uses of blockchain technology beyond transferring value. Any statement or transaction can be recorded on a blockchain and can take advantage of its properties. For instance, student activists in China have published essays on Ethereum's blockchain to circumvent the state's censorship of their letters.[3] A blockchain-like structure is used to store auditable records of domain ownership for encrypting internet traffic.[4] Blockchains can also potentially be used to record and transfer property and manage public records.

Blockchain technologies (such as cryptocurrencies) have the potential to enhance civil liberties by importing some of the civil liberties protections that citizens enjoy offline into the digital world. For example, Zcash combines recent cryptographic innovations with blockchain technology to enable private transactions using digital currency. Decentralized technologies are also more resistant to corporate censorship by existing financial institutions, which have a long history of shutting down the accounts of individuals engaged in legal but controversial speech.[5] These goals are not new; blockchain technologies simply import these attributes of cash—anonymity and resistance to censorship—into the online world.

Blockchain technologies also include so-called "smart contracts," which enable the automatic execution of more complex transactions, like submitting bids in an auction, without necessarily requiring the involvement of intermediaries. Smart contracts are executed by all parties who validate transactions to ensure the blockchain's integrity. Smart contracts are a new technology that may have significant implications for improving the reliability and security of many financial protocols such as auctions, asset exchanges, and insurance.

---

[3] *See* Josh Horowitz, *#MeToo Activists in China Are Turning to the Blockchain to Dodge Censorship*, https://qz.com/1260191/metoo-activists-in-china-are-turning-to-the-blockchain-to-dodge-censorship/.

[4] *See Certificate Transparency*, https://www.certificate-transparency.org/.

[5] *See Financial Censorship*, EFF.org, https://www.eff.org/issues/financial-censorship.

To perform a transaction on a blockchain (such as transferring cryptocurrency from one user to another), users must acquire the relevant digital currency. For example, to send Bitcoin to another user on the Bitcoin blockchain, a user would first need to acquire Bitcoin. This can be done by "mining" the currency (that is, contributing resources to the decentralized network in exchange for the possibility of obtaining some amount of the currency) or buying the native currency with some other currency (such as U.S. dollars). Mining is not always feasible for individuals, so many people obtain digital currencies through centralized exchanges. Blockchains themselves are decentralized, and transactions on blockchains are resistant to censorship. However, centralized exchanges act as choke-points through which users must pass to begin participating in the network; thus, financial censorship is most easily conducted at centralized exchanges.

We have already seen examples of centralized exchanges mishandling user funds and betraying the trust of customers. Centralized exchanges can freeze the funds of customers, block certain customers from the platform, or block specific transactions, with no obligations to provide affected customers with an appeals process. Centralized exchanges can suffer outages, hacks, or losses that prevent customers from accessing their digital currencies.[6] These centralized exchanges are also a target for criminals seeking to steal customer funds, and can themselves be run by unscrupulous individuals who abuse their access to customer funds and data.[7]

Decentralized exchanges, by contrast, allow for the exchange of digital currencies using smart contracts. For example, requests to sell and purchase cryptocurrency can be submitted to a smart contract that matches and completes these exchange transactions. Decentralized exchanges generally do not need to hold funds for customers—rather, customers maintain possession of their cryptocurrency, and the decentralized exchange can automatically execute exchange transactions without taking possession of the assets. Decentralized exchanges thus generally do not possess a central honeypot of money that might attract criminals like centralized exchanges do, and cannot themselves steal funds. Since smart contracts are executed by global, non-colluding parties, no one party can approve, control, or restrict the execution of a decentralized exchange transaction. Because trades are not approved by an individual or group, they cannot be easily censored by a single entity.

Decentralized exchanges are in their earliest stages of development, and it is not our intention in this letter to analyze whether EtherDelta itself was fully decentralized or

---

[6] *See* Karen Zraick, *Crypto-Exchange Says It Can't Pay Investors Because Its C.E.O. Died, and He Had the Passwords*, The New York Times (Feb. 5, 2019), *https://www.nytimes.com/2019/02/05/business/quadriga-cx-gerald-cotten.html*.

[7] *See Daily Report: Mt. Gox, Having Lost Essentially All Bitcoins, Files for Bankruptcy*, The New York Times (Feb. 28, 2014), https://bits.blogs.nytimes.com/2014/02/28/daily-report-mt-gox-having-lost-essentially-all-bitcoins-files-for-bankruptcy/.

whether factors beyond the exchange's published code should have drawn regulatory scrutiny. But this is an area of rapid research and innovation, and many cryptographers and programmers are experimenting with other trustless smart contract applications that may have significant public benefit in the long term.

IV. The SEC's Statements, Without Clarification, Suggest Legal Standards that Would Violate the First Amendment

The SEC's broad language could be read to imply that anyone merely writing and publishing code that becomes part of a decentralized exchange could be subject to licensing requirements or liability. Because publishing code is constitutionally protected speech, requiring a license to exercise the First Amendment right of writing and publishing computer code would be an unconstitutional prior restraint on speech, and imposing regulatory or criminal liability for such activity would also run afoul of the First Amendment.

A. Computer Code Is Constitutionally Protected Speech

Courts have long recognized that computer code is speech protected by the First Amendment. *Universal City Studios, Inc. v. Corley,* 273 F.3d 429,445-46 (2d Cir. 2001); *Jungerv. Daley,* 209 F.3d 481,485 (6th Cir. 2000); *Bernstein v. Dep't of Justice,* 176 F.3d 1132,1140-41 (9th Cir. 1999), *reh'g granted, opinion withdrawn,* 192 F.3d 1308 (9th Cir. 1999); *Karn* v. *Dep't of State,* 925 F. Supp. 1,9-10 (D.D.C. 1996).

As the Second Circuit explained in *Corley*:

> Instructions such as computer code, which are intended to be executable by a computer, will often convey information capable of comprehension and assessment by a human being. A programmer reading a program learns information about instructing a computer, and might use this information to improve personal programming skills and perhaps the craft of programming. Moreover, programmers communicating ideas to one another almost inevitably communicate in code, much as musicians use notes. . . . Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both).

273 F.3d at 448.

Smart contract code on public blockchains are publicly viewable and often open source, which means anyone can read the code, understand how it works, test it, suggest improvements, and alert others to potential code vulnerabilities. This discourse is vital to research and development efforts that benefit the public. Additionally, the transparency of the code helps to ensure that the code will function securely and be free of malicious

or biased behavior. Many decentralized exchanges have open-sourced and published their code for this reason.

B. The First Amendment Also Protects Financial Transactions

In addition to the fact that the code behind decentralized exchanges is itself speech, decentralized exchanges also foster freedom of association by allowing for pseudonymous transactions that are resistant to censorship. *See NAACP v. State of Alabama ex rel. Patterson,* 357 U.S. 449,460-62 (1958). Protection of such financial transactions is critical to ensuring public access to speech, as the ability to collect funds often plays a near-existential role in expression, online and offline.

Censorship is often effectuated through financial means. As just one example, in *Backpage.com, LLC v. Dart*, a county sheriff "embarked on a campaign intended to crush" a web page "by demanding that firms such as Visa and MasterCard prohibit the use of their credit cards to purchase any ads" on the website. 807 F.3d 229, 230 (7th Cir. 2015). Visa and MasterCard "bowed to pressure … by refusing to process transactions in which their credit cards are used to purchase any ads on [the website], even those that advertise indisputably legal activities." The Seventh Circuit held that the sheriff's conduct violated the First Amendment, describing how the sheriff proceeded against the website "not by litigation but instead by suffocation, depriving the company of ad revenues by scaring off its payments-service providers. The analogy is to killing a person by cutting off his oxygen supply rather than by shooting him." *Id.*

Similarly, technologies that allow for peer-to-peer transactions without an intermediary protect against censorship by eliminating the potential choke-point.

C. Requiring a License to Write and Publish Code Would Be an Unconstitutional Prior Restraint on Speech

The SEC's broad language arguably implied that the researchers and programmers experimenting with trustless smart contracts and innovative tools for future decentralized exchanges could be expected to register to operate a securities exchange, even if these individuals never deployed the code, and never actively ran or promoted a decentralized exchange. The free speech protections enshrined in the First Amendment and upheld through court cases across decades include the rights of individuals to publish their ideas without preemptively obtaining a license. Forcing researchers to obtain a license prior to publishing their code, or describing their methods in a white paper, would unconstitutionally hamper the expressive rights of countless coders and researchers in this space.

A prior restraint on speech is invalid unless it survives the most exacting scrutiny. *Org. for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971) ("Any prior restraint on expression comes … with a heavy presumption against its constitutional validity" and "varies a

heavy burden of showing justification") (internal quotation marks omitted). Prior restraints are justified only in unusual and extreme circumstances, when no other remedy will suffice. *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). Under *Nebraska Press*, prior restraints must be "necessary" to further a governmental interest of the highest magnitude. *Id.* at 562-563. A prior restraint is necessary only if (1) the harm to the governmental interest is highly likely to occur, (2) the harm will be irreparable; and (3) no alternative exists for preventing the harm. *See Nebraska Press* at 563-567; *see also New York Times v. U.S.* 713, 730 (1971) (Stewart, J. concurring); *Levien v. U.S. Dist. Ct.*, 764 F.2d 590, 595 (9th Cir. 1985).

In addition, *Freedman v. Maryland* places strict limits on the duration and manner of prior restraints unilaterally imposed by executive officials. 380 U.S. 51 (1965). In *Freedman*, the Supreme Court held that any administrative scheme requiring governmental permission before one can speak must have built into it three core procedural protections ensuring prompt and searching judicial review: (1) any restraint imposed prior to judicial review must be limited to "a specified brief period"; (2) after review is initiated, the period of restraint before final judicial determination must be limited to "the shortest fixed period compatible with sound judicial resolution"; and (3) the burden of going to court to suppress speech and the burden of proof in court must be placed on the government. *Freedman*, 380 U.S. at 58-59.

A licensing scheme that restricted the ability to merely write and publish code would fail the exacting test for prior restraints set forth in *Nebraska Press*, or, at minimum, would likely fail to comply with the procedural requirements in *Freedman v. Maryland*.

D. Imposing After-the-Fact Liability for Writing and Publishing Code Would Also Violate the First Amendment

It is crucial that those engaged in developing protocols, verifying transactions through mining, and writing code should not be held liable for operating or assisting with operating a securities exchange. Imposing regulatory or criminal liability for such activity would also run afoul of the First Amendment.

The SEC's language that Coburn "should have known" that writing and deploying the EtherDelta smart contract to the Ethereum Blockchain "would contribute to EtherDelta's violations" and thus that Coburn "caused EtherDelta to violate Section 5 of the Exchange Act" suggests a legal standard that contradicts the First Amendment's standard of intent. The First Amendment generally bars claims against publishers for inciting harmful conduct via the knowing publication of motivational or instructional speech. Courts have held that publishers can only be held liable for content that results in death or bodily injury in cases where (i) the publisher has the specific intent to encourage the commission of violent acts, and (ii) the publisher provides specific instructions to commit the acts, rather than abstract advocacy. *See Rice v. Paladin Enters.*, 128 F.3d 233, 242 (4th Cir. 1997); *Herceg v. Hustler Magazine, Inc.*, 814 F.2d 1017, 1021–22 (5th Cir. 1987)

(overturning jury verdict against publisher because there was no evidence that the publisher intended, advocated for, or directly incited teen to engage in dangerous behavior); *Corley*, 273 F.3d at 447 n.18 (2d Cir. 2001) (noting that even publication of instructions on how to commit illegal acts are subject to First Amendment scrutiny); *James v. Meow Media, Inc.*, 300 F.3d 683, 695, 699 (6th Cir. 2002) (refusing to hold video game, movie, and Internet companies liable for murder of students by fellow classmate, stating "attaching tort liability to the effect that such ideas have on a criminal actor would raise significant constitutional problems under the First Amendment"); *cf. See Brandenburg v. Ohio,* 395 U.S. 444, 447 (1969) ("constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action").

Imposing criminal or regulatory liability on programmers who "should have known" that their code may be used in a particular way would run afoul of the First Amendment.

E. The SEC's Language Could Chill Blockchain Innovation, Even Beyond Decentralized Exchanges

The SEC's broad language might lead to widespread confusion and fear among those who develop and maintain the platforms used by decentralized exchanges, discouraging innovation. For example, the SEC's statement included the example that "if one entity arranges for other entities, either directly or indirectly, to provide the various functions of a trading system that together meet the definition of an exchange, the entity arranging the collective efforts could be considered to have established an exchange." The concept of indirectly arranging for an entity to provide "various functions" of a trading system could be read to encompass developers working to create and maintain protocols that are later utilized by decentralized exchanges as well as miners working to verify transactions that execute smart contracts.

Decentralized systems are also the topic of a great deal of academic and industry research, and the SEC's language may chill further discourse. As the Second Circuit explained in *Corley*: "Limiting First Amendment protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars, just as limiting protection for musicians to descriptions of musical scores (but not sequences of notes) would impede their exchange of ideas and expression." *Corley*, 273 F.3d at 448.

EFF urges the SEC to clarify that it recognizes that merely writing and publishing code is constitutionally protected, in order to ensure that blockchain innovation can continue to thrive.

Sincerely,

Rainey Reitman
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
415-436-9333
rainey@eff.org