Assembly California Legislature

Assembly Committee on Banking and Finance

Informational Hearing of the Assembly Committee on Banking and Finance and Select Committee on Technological Advances

Virtual Currency Businesses: The Market and Regulatory Issues

Testimony of Rainey Reitman
Chief Program Officer
Electronic Frontier Foundation

October 17, 2019

Thank you for the opportunity to testify about the potential regulation of blockchain technologies in the state of California. I represent the Electronic Frontier Foundation, a non-profit civil liberties law and technology organization. Founded in 1990, EFF champions privacy, free expression, and innovation. We have over 30,000 dues-paying members. The majority of EFF's funding comes from these individual people, and that is because our mandate is to represent the concerns of technology users, both today's technology users and tomorrow's.

I am the Chief Program Officer of EFF, and I have written and spoken publicly about the civil liberties implications of blockchain technology and its potential regulation since 2011.

I am honored to speak with you about this issue today. As the California legislature considers potential regulation of blockchain, I would like to offer a few thoughts to help frame the conversation.

First, policymakers should note that the impetus behind blockchain technologies is one that seeks to empower consumers in financial systems where they have been historically and systematically disempowered and robbed of their privacy. In my role at EFF, I have been contacted by individuals and small businesses many times over the years who have had their financial accounts and payment systems restricted or shut down with little recourse, based on the whims of banking institutions rather than on the execution of laws. For example, Smashwords is one of the world's most popular hubs for self-published authors, and pays all their authors through PayPal. PayPal shut down their entire account[1] because some of their romantic fiction—to be clear, books of fiction with no photos—was too risqué for PayPal's tastes. With companies like Wells Fargo fraudulently opening millions of accounts and Equifax exposing the sensitive data of over 148 million Americans, American consumers have more reason than ever to be wary of sharing their financial information. Many blockchain innovations seek to use technology to protect the privacy and security of consumer data—and to keep financial information away from corporations that have proven they cannot be trusted with it.

While blockchain technologies alone cannot resolve this disempowerment, technological advances such as blockchain may well prove part of long-term solutions that empower technology consumers. Policymakers should view many blockchain innovations as a technological partner in the regulatory fight to defend consumers against wrongdoing by financial companies.

Secondly, policymakers should know that the human rights of privacy and freedom of expression are heavily implicated by many of the potential regulations of blockchain technology. For example,

---

[1] Rainey Reitman, *Legal Censorship: PayPal Makes a Habit of Deciding What Users Can Read,* Electronic Frontier Found. (Aug. 21, 2018). Retrieved from https://www.eff.org/deeplinks/2012/02/legal-censorship-paypal-makes-habit-deciding-what-users-can-read.

EFF has pushed back against proposals that would prevent everyday technology users from protecting their financial transactions using privacy coins, or tokens that protect the privacy of their users.[2] We have also opposed proposals to regulate or ban the publication of open source software.[3] Attempting to prevent consumers from accessing technology that protects their individual privacy or from publishing free software raises a host of human rights issues, in addition to being contrary to the free speech and privacy protections enshrined in the Constitution.

A blockchain is a distributed ledger—a database that stores multiple copies of data across many computers in a network.[4] The first application of blockchain technology was Bitcoin. Bitcoin's promise was to revolutionize value as the Internet revolutionized information—to make it possible to send value across the globe digitally and securely, without needing a bank.

Traditionally, transferring values between parties required third parties like banks that maintained ledgers of transactions. Bitcoin cut out the multiple intermediaries that needed to update their ledgers and coordinate with each to process transactions, in favor of a single ledger that permanently records every transaction. That ledger is not maintained by a single entity, but rather stored and maintained by many computers working together in a network. [5] This "distributed

---

[2] "Privacy coin" is a general term used to refer to a range of different blockchain-based tokens that have built-in protections for transactional privacy. Using cryptography, these privacy coins are designed to publicly verify transactions while not revealing the identity of the sender, the receiver, or the transaction amount. Two well-known privacy coins are ZCash and Monero. J. Frankenfield, *Zcash*, Investopedia (Mar. 12, 2019). Retrieved October 14, 2019, from https://www.investopedia.com/terms/z/zcash.asp.; J. Frankenfield, *Monero*, Investopedia (Mar. 12, 2019). Retrieved October 14, 2019, from https://www.investopedia.com/terms/m/monero.asp.

[3] Open source software is software that is published freely, so that anyone can make a copy, edit, or contribute to it. This so-called "free software" has been widely adopted and is now a primary, common form of expression for ideas that are implemented in software. Today, it is used widely across the Internet and Linux, the primary operating system used on Internet servers and which underlies the Android mobile operating system, continues to be maintained as a free software project contributed to by thousands of commercial companies, and tens of thousands of individual developers, volunteers, and academics. Read more about EFF's recent comments to HM Treasury describing the impact of banning the publication of open source software as part of blockchain regulation. Rainey Reitman, *EFF and Open Rights Group Defend the Right to Publish Open Source Software to the UK Government*, Electronic Frontier Found. (Aug. 16, 2019). Retrieved from https://www.eff.org/deeplinks/2019/06/eff-and-open-rights-group-defend-right-publish-open-source-software-uk-government.

[4] The National Institute of Standards and Technology defines "blockchains" as "[i]mmutable digital ledger systems implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority. At its most basic level, they enable a community of users to record transactions in a ledger public to that community such that no transaction can be changed once published." Dylan Yaga, et al., *Blockchain Technology Overview*, NAT'L INST. OF STANDARDS AND TECH. (Oct. 2018), available at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

[5] "A blockchain can be public or private. In a public blockchain, anyone can create a public-private key pair and download a copy of the blockchain. . . . In a private blockchain, the membership of users on the

ledger" is called a "blockchain," because the ledger permanently and securely stores data by linking (or "chaining") blocks of data together through encryption.

The Bitcoin blockchain is a record of Bitcoin transactions,[6] but there are many other applications of this distributed ledger technology. As the legislature thinks about regulation, it is vital to recognize that future innovation in this space might be using these distributed ledgers for purposes beyond what we typically think of when we think of financial services.

One example is Filecoin, which applies blockchain technology to file storage. The legislature may remember a few months ago when huge swaths of the Internet—including popularly used tools like Slack and Github—were unavailable for hours.[7] That is because so much of the modern web are using a single service to store their data: Amazon Web Services. When an Amazon data center suffered an outage for several hours, multiple popular online platforms were unavailable to consumers. Filecoin seeks to decentralize file storage so that there is no single point of failure like the current system that is so heavily reliant on Amazon Web Services. Any one of Amazon's many smaller storage competitors or potentially even technically-minded individuals could offer storage through the same protocol, and the transactions made between application developers and these storage providers would be recorded on a blockchain.

While we cannot yet know how successful services like Filecoin will ultimately be, I offer it as an example of a blockchain project designed to serve consumer needs that are not met by modern tech companies, and that create a more decentralized—and therefore more resilient—web. As the legislature considers how to proceed, I urge you to keep front and center the interests of technology

---

blockchain is controlled. A blockchain can be permissioned or permissionless, which is independent of whether the blockchain is public or private. A permissioned blockchain is one in which the permission of a user is assigned to them. . . . In a permissionless blockchain, all users have equal rights, with any one able to download the full blockchain and have an opportunity to potentially add additional blocks." Chris Jaikaran, *Blockchain: Background and Policy Issues*, Cong. Research Serv., R45116 (Feb. 28, 2018).

[6] The Bitcoin blockchain is the ledger that records Bitcoin transactions. Each "entry" in the ledger records a transaction, showing the "public key" (a string of numbers and letters similar to a username) of the user sending the Bitcoin and the user receiving the Bitcoin, the amount of Bitcoin being sent, and the time of the transaction. Each "public key" is associated with a "private key" (similar to a password) that enables the user associated with that public key to transfer the Bitcoin to other users. To "own" Bitcoin is simply to know the private key associated with a public key that has received Bitcoin.

[7] J. Swearingen, *When Amazon Web Services Goes Down, So Does a Lot of the Web*, New York Magazine (Mar. 2, 2018). Retrieved October 14, 2019, from http://nymag.com/intelligencer/2018/03/when-amazon-web-services-goes-down-so-does-a-lot-of-the-web.html.; C. Newton, *How a typo took down S3, the backbone of the internet*. The Verge (Mar. 2, 2017). Retrieved October 14, 2019, from https://www.theverge.com/2017/3/2/14792442/amazon-s3-outage-cause-typo-internet-server.

users, especially those under-served by existing technology companies who may benefit from future innovation.

EFF has developed a set of guiding principles to help regulators balance the needs for innovation, consumer choice, and consumer protection.

To summarize these principles:

Principle 1: Regulation should not undermine privacy-enhancing innovation in this space. The right to privacy is enshrined in the United States Constitution, in international human rights law, and in California's own Constitution. This state has long been a leader in defending consumer privacy and a bellwether state for bringing new privacy protections to consumers. California must uphold these consumer protections in the cryptocurrency space, ensuring that new innovations to defend consumer privacy can flourish.

Principle 2: Regulation should not chill future technological innovation that will benefit consumers. Though the blockchain ecosystem is still relatively young, there are already well-established companies with the resources to hire expert counsel and compliance officers to navigate state, federal, and international regulations. We want to ensure that these early entrants do not establish themselves and then pull up the ladder behind them. In the technology sphere, when existing services do not serve the needs of consumers, innovative new products come along to try to give consumers better choices. We must ensure that new services can continue to be created to serve all consumers, and that we do not merely entrench the big companies of today. As regulators enter this space, they should ensure generous on-ramps to give new services the time to build their products and find their market before having to navigate onerous regulatory burdens.

One important piece of this is ensuring regulations are technologically neutral. Attempts to write laws to capture the technological details of one specific cryptocurrency could have massive and unintended impacts on the market, such as prioritizing one type of technical solution over others or driving innovation away from a particular method of doing something.

Principle 3: Regulation should focus on custodial services. Custodial services—those entities that hold and trade tokens on behalf of users—are most likely to abuse consumer trust. In fact, they have already developed a sordid history of fraud and sloppy security practices. These companies need to be held accountable to ensure that they cannot defraud consumers. Regulators should focus their energies on crafting regulation that holds these bad actors that offer custodial services to account**.**

This includes ensuring that any regulation protects individual miners, merchants who accept cryptocurrencies, and individuals who trade in cryptocurrency as consumers**.** Cryptocurrency miners merely confirm transaction and maintain copies of a blockchain, offering computing power

to keep the network healthy and functional. They do not offer direct services to consumers and should be neutral actors—verifying but not interrupting or prioritizing any transactions. At this stage in blockchain's development, there is no reason for regulators to put compliance or regulatory burdens on miners. Similarly, everyday merchants who are offering consumers new choices by accepting cryptocurrencies for purchases, and consumers who are experimenting with using cryptocurrencies for commerce should not be burdened by additional regulation at this time.

Principle 4: Any regulation should recognize the important role of decentralized exchanges and other decentralized technologies in empowering consumers. Centralization of control creates brittle digital systems where a single point of failure can shut down commerce or communication. Much of the strength of the modern web comes from its decentralization—and many of the problems we see in technology space are a result of a handful of big technology companies having undue control over much of our digital experience. Blockchain technologies were built to be resilient and decentralized, and future innovation that advances decentralization – including decentralized exchanges – should be protected.

Principle 5: Regulations should not punish those who merely write and publish code. EFF fought to establish, and several courts have recognized, that writing code is a form of expressing ideas, similar to other forms of communication like writing music or books and thus is protected by the First Amendment. Policymakers must ensure that regulations aimed at blockchain technologies do not prohibit the publication or distribution of code or otherwise require parties to obtain a government license before publishing or distributing their code.

Thank you for allowing me to share my thoughts with you today. I look forward to continuing the discussion.