COIN CENTER

PRINCIPLES FOR CRYPTO LEGISLATION

An introduction to crypto and principles for protecting American rights and innovation.

Peter Van Valkenburgh, with articles by Jerry Brito

DIGITAL COPY WITH ALL LINKS AVAILABLE HERE:

coincenter.org/principles-legislation

ABSTRACT

A general introduction to “crypto,” both the underlying technology as well as the larger ecosystem, and a set of principles for legislating in this area to ensure that American rights are protected and American innovation is able to flourish.

AUTHOR

Peter Van Valkenburgh
Executive Director of Coin Center
peter@coincenter.org

ACKNOWLEDGEMENTS

Thank you to my Coin Center colleagues Neeraj Agrawal, Antonie Hodge, Landon Zinda, Robin Weisman, Andrea O’Sullivan, Alex Sternhell, Mike Ahern, and Jerry Brito for indispensable discussions, comments, and 10 years of hard work that have led to this and so much more.

TABLE OF CONTENTS

WRITING A DESCRIPTION FOR THIS THING FOR GENERAL AUDIENCES IS BLOODY HARD. THERE’S NOTHING TO RELATE IT TO.

— SATOSHI NAKAMOTO

INTRODUCTION

This guide is intended for Congressional staff and members who are working on crypto policy. Whether you have been working in this area for some time, or are new to crypto, lawmaking, or both, our aim is to create a resource for sound policy decisions based on our 10 years of experience.

But who are we? Coin Center's mission is to defend the rights of individuals to build and use free and open cryptocurrency networks: the right to write and publish code—to read and to run it. The right to assemble into peer-to-peer networks. And the right to do all this privately. We do this by producing and publishing policy research, educating policymakers and the media about cryptocurrencies, advocating for sound public policy, and by engaging in litigation to defend digital civil liberties.

We are not a trade association and do not represent the interests of any businesses that are building on top of crypto. Instead, our goal is to represent and defend the underlying technology itself as a public good: a series of free and open tools and networks through which anyone can control their own assets and transactions, and upon which anyone is free to innovate and build.

A complex and technical subject, "crypto" can mean a lot of different things to a lot of different people. Getting a fair lay of that land can be tough. Part I will explain "crypto," both the technology and the ecosystem, and flag important distinctions that will be critical for lawmakers when faced with policy decisions. Part II will explore ten principles for drafting law in this space. We thank you and your office for learning about these important technologies and exercising care when making important decisions affecting the safety, opportunity, and prosperity of Americans transacting and building on the electronic financial frontier.

PART I: “CRYPTO”

“Crypto” is an emergent technological phenomenon, like the Internet, so there’s no authoritative definition of the term. Today, “crypto” is used to describe a broad category of innovations and consequent individual and business activities that stem from an original invention, Bitcoin and its blockchain.

If you are confidently familiar with Bitcoin, the next section may be something you skip or skim; the important thing to remember is that Bitcoin is the world’s first completely decentralized, open-source, and peer-to-peer digital currency. Everything in “crypto,” which we’ll return to in a moment, begins with that.

BACKGROUNDER: WHAT ARE BITCOIN AND CRYPTOCURRENCIES?

BY JERRY BRITO

To understand cryptocurrency, it’s best to start with the most popular and in many ways the simplest of these networks: Bitcoin

Bitcoin is the world’s first completely decentralized, open-source, and peer-to-peer digital currency. A short decade ago, knowledge of it was confined to a handful of hobbyists on Internet forums. Today, the Bitcoin economy is larger than the economies of some of the world’s smaller nations. The value of a bitcoin (or BTC) has grown and fluctuated greatly, from pennies to many tens of thousands of dollars.

NO THIRD PARTIES

Bitcoin is the world’s first completely decentralized, open-source, and peer-to-peer digital currency. Until Bitcoin’s invention in 2008 by the unidentified programmer known as Satoshi Nakamoto, online transactions always required a trusted third-party intermediary. For example, if Alice wanted to send $100 to Bob over the Internet, she would have had to rely on a third-party service like PayPal or MasterCard. Intermediaries like PayPal keep a ledger of account holders’ balances. When Alice sends Bob $100, PayPal deducts the amount from her account and adds it to Bob’s account. Without such intermediaries, digital money could be spent twice. Imagine there are no intermediaries with ledgers, and digital cash is simply a computer file, just as digital documents are computer files. Alice could send $100 to Bob by attaching a money file to a message. But just as with email, sending an attachment does not remove it from one's computer. Alice would retain a copy of the money file after she sends it. She could then easily send the same $100 to Charlie. In computer science, this is known as the "double-spending" problem and until Bitcoin, it could only be solved by employing a trusted ledger-keeping third party. Bitcoin's invention is revolutionary because, for the first time, the double-spending problem can be solved without a third party.

PEER-TO-PEER

Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network. Every transaction that occurs in the Bitcoin economy is registered in a publicly distributed ledger, which is called the blockchain. New transactions are checked against the blockchain to ensure that the same bitcoins haven't already been spent, thus eliminating the double-spending problem. The global peer-to-peer network, composed of thousands of users, takes the place of an intermediary; Alice and Bob can transact without PayPal. One thing to note right away is that transactions on the Bitcoin network are not denominated in dollars or euros or yen as they are on PayPal, but are instead denominated in bitcoins. This makes it a virtual currency in addition to a decentralized payments network.
The value of the currency is not derived from gold or government fiat, but from the value that people assign to it. The dollar value of a bitcoin is determined on an open market, just like the exchange rate between different world currencies.

ELECTRONIC CASH

Bitcoin is not the first permissionless, decentralized, peer-to-peer payments technology in the world. Paper cash is. If someone hands you a banknote, that is a settled transaction. There are no intermediaries and no one knows about it but the two parties involved. Until now, it has been unfortunately necessary to include a third party to make these transactions online. And those third parties see everything.

What makes Bitcoin remarkable is that it is the first Internet payment system that resembles physical cash. Now, instead of being limited to using cash only with people whom you interact with face to face, or taking the chance on mailing bills, you can send digital cash in the form of Bitcoin to anyone in the world.

There have been countless attempts to build on the Bitcoin system we've just described. Technologists have been experimenting with ways to build functionality into the Bitcoin network, or have opted to try to build entirely new networks built with similar decentralized designs and native tokens. These projects have given us hundreds of other cryptocurrencies. Their developers are testing a host of experimental new features, such as sophisticated programming languages, enhanced privacy, different forms of mining, and much more.

"CRYPTO" AS A BROADER INTEREST GROUP

The Cambrian explosion of innovations and businesses that built on top of Bitcoin's original invention are what we would broadly call "crypto" today. These include entirely **new cryptocurrencies**, which have their own blockchains and native assets, like Ethereum, Zcash, and Solana. These also include substantial projects to scale or increase the functionality of underlying cryptocurrency networks, like Bitcoin's Lightning Network, or any of the several **"layer 2" projects** aiming to scale Ethereum (e.g. Arbitrum, Optimism, and Starknet).

Crypto is also sometimes used to refer to businesses built on top of these technologies. Those businesses include professional **miners** and **stakers**, who create new blocks on cryptocurrency networks and earn associated rewards and fees. Other businesses offer to hold and safekeep cryptocurrency on behalf of their customers and may facilitate buying, selling, or trading cryptocurrencies; these businesses are referred to as **custodial wallets** and **exchanges**. Still other crypto businesses may specialize in issuing and redeeming dollar-backed tokens that are transferable on cryptocurrency networks, known as **stablecoins**.

More recently, many of the cryptocurrency services that once required an intermediary business, like custodial exchange and trading services, can now be performed solely by an individual using blockchain-based software, which is somewhat confusingly called **"smart contracts."** These smart contract applications may allow for direct, peer-to-peer trading (i.e. decentralized exchange); lending; collectible trading (i.e. non-fungible tokens or **NFTs**); stablecoin issuance (algorithmic or **decentralized stablecoins**); and a host of other financial and non-financial activities. Broadly speaking, these tools are referred to as **DeFi** (i.e. decentralized finance). However, depending on how the software is written and maintained, these tools may fit a number of other important distinctions. They may be **non-custodial**; meaning no human aside from the user has control over the funds. They may be **immutable**; which means that once published to the blockchain, the software and its associated functionality can never be changed. Then there are distinctions to be made regarding their **governance**, or the decisions over how to maintain, change, and upgrade the software. DeFi tools may exhibit **decentralized governance**, which is a contentious term for the number of independent persons involved in decision making and the technological limitations that prevent some subset of those persons from controlling the fate of the project or the user assets it handles.

Finally, crypto can also refer to the communities of people and businesses who develop, maintain, publish, and use the underlying software that makes cryptocurrency networks and applications possible. If these developers work directly on software for a particular cryptocurrency's basic functionality, then we call them **core devs.** If they work on software for decentralized finance tools we may call them **smart contract devs**. Most legitimate cryptocurrency software is published **open source,** which means that anyone can use it and modify it without seeking a license or other permission from the original developers. Some crypto developers work on their own on these projects; others may work for a company dedicated purely to software development; still others may work for a company that does software development but also performs trusted services like custodial wallets or exchanges.

When someone approaches your office about "crypto," they very well could come from any of these highly diverse sub-categories of "crypto." They may be an individual or a company. Their company may be in a position of trust vis-à-vis their customers' finances (akin to a bank) or their company may simply be a software development and publishing operation that provides tools for individuals to control their own assets and financial activities (akin to a physical safe or armored car manufacturer).

CONCLUSION TO PART I

In Part I of this guide, we've offered you a basic overview of crypto, covering both the fundamental value of the technology as well as the diverse range of interests, follow-on innovations, and businesses that make up the broad category of "crypto" today. As with any complex topic, there are a myriad of details that we have omitted. At coincenter.org, you will find many more backgrounders and reports delving into detailed aspects of the technology and associated ecosystem. For a firmer understanding of the underlying tech, we recommend: "What is a blockchain anyway?";[1] "What is Bitcoin mining, and why is it necessary?";[2] and "What is 'open source' and why is it important?".[3]

To better understand the value of these technologies, check out: "What is cryptocurrency good for?";[4] "What does 'permissionless' mean?";[5] and our long form report "Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet."[6]

To explore new frontiers of crypto beyond Bitcoin, see: "What is 'staking'?";[7] "What are mixers and 'privacy coins'?";[8] and "How does Tornado Cash work?,"[9] which we recommend as a deep dive into a particular smart contract-based privacy tool that's highly relevant in ongoing litigation and policy debates.

[1] Peter Van Valkenburgh, "What is a blockchain anyway?" *Coin Center,* April 25, 2017, https://www.coincenter.org/education/blockchain-101/whats-a-blockchain/.

[2] Peter Van Valkenburgh, "What is Bitcoin mining, and why is it necessary?," *Coin Center,* December 15, 2014, https://www.coincenter.org/education/advanced-topics/mining/.

[3] Peter Van Valkenburgh, "What is 'open source' and why is it important?," *Coin Center*, October 17, 2017, https://www.coincenter.org/education/advanced-topics/open-source/.

[4] Andrea O'Sullivan, "What is cryptocurrency good for?" *Coin Center,* July 30, 2018, https://www.coincenter.org/education/blockchain-101/what-is-cryptocurrency-good-for/.

[5] Peter Van Valkenburgh, "What does 'permissionless' mean?" *Coin Center,* January 31, 2017, https://www.coincenter.org/education/advanced-topics/what-does-permissionless-mean/.

[6] Peter Van Valkenburgh, "Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet," *Coin Center,* December 2016, https://www.coincenter.org/open-matters-why-permissionless-blockchains-are-essential-to-the-future-of-the-internet/.

[7] Peter Van Valkenburgh, "What is 'staking'?" *Coin Center,* January 24, 2022, https://www.coincenter.org/education/advanced-topics/what-is-staking/.

[8] Andrea O'Sullivan, "What are mixers and 'privacy coins'?" *Coin Center,* July 7, 2020, https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/.

[9] Alex Wade, Michael Lewellen, and Peter Van Valkenburgh, "How does Tornado Cash work?" *Coin Center*, August 25, 2022, https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/.

PART II: CRYPTO AND PUBLIC POLICY

In Part II, we'll begin with an overview of the existing regulatory landscape and then proceed to outline our ten principles for drafting effective and constitutional legislation. To start, we'll look at a foundational question, often misunderstood by those new to the topic: Is Bitcoin regulated? If you've been working in this space for some time, you may already know the answer; you might have already read this backgrounder, first published by Coin Center in 2014! If so, feel free to skim or skip to the principles in the next section; if you are new to the space, there's still great value in starting with the following fundamental question.

BACKGROUNDER: IS BITCOIN REGULATED?

BY JERRY BRITO

Is Bitcoin Regulated? Yes. It is.

A common misconception about Bitcoin and other cryptocurrencies is that they are not regulated. The claim is frequently repeated in the media:

> *"The so far unregulated digital currency has courted controversy because of its volatile value and its popularity among cybercriminals."*
>
> *– BBC News, August 15, 2014*[10]

> *"The value in the decentralized and unregulated digital currency has plummeted since hitting a high of more than $1,130 in December 2013."*

[10] Zoe Kleinman, "Retailers look to Bitcoin as currency for life's basics," *BBC News,* August 15, 2014, https://www.bbc.com/news/technology-28802887.

> *– USA Today, October 22, 2014*[11]

> *"A Texas man was charged with fraud in New York on Thursday, in what federal authorities claim is the first-ever Ponzi scheme involving the unregulated digital currency Bitcoin."*
>
> *– TIME, Nov. 6, 2014*[12]

That last one is pretty telling. If the use of Bitcoin in certain circumstances wasn't regulated, what was the Texas man arrested for?

The truth is that a wide variety of laws and regulations have applied to the use of Bitcoin since its inception in 2009. The confusion seems to stem from the idea that, because governments have not taken steps to regulate the currency specifically, it is therefore unregulated. Using the U.S. legal context as an example, this backgrounder will show that it is not really accurate to say that Bitcoin is an unregulated digital currency.

NETWORK VS. ACTORS

Part of the problem with saying that Bitcoin is unregulated is that it's not often clear what is meant by "Bitcoin." Do we mean the technology, the peer-to-peer network, or individual use of that network in commerce?

In some sense it may be accurate to say that the technology and the peer-to-peer network are unregulated. In fact, these may be beyond regulation. The technology is ultimately a protocol—a set of shared rules that can be expressed in writing—so it is protected speech, not subject to prior restraint under the First Amendment, except in rare cases of compelling governmental interest. And the peer-to-peer network as a whole is practically impossible to regulate because it is decentralized—too many participants to police efficiently, and many outside of U.S. jurisdiction altogether.

[11] Mike Snider, "Bitcoin may be volatile but has value beyond price point," *USA Today,* October 22, 2014, https://www.usatoday.com/story/tech/2014/10/22/bitcoin-update-not-as-shiny/17669785/.

[12] Rishi Iyengar, "Man Accused of Running the First Ever Bitcoin Ponzi Scheme," *TIME*, November 6, 2014, https://time.com/3571415/bitcoin-ponzi-scheme-trendon-shavers-bitcoin-savings-and-trust/.

In another, perhaps more pedantic, sense, however, it may be more accurate to say that Bitcoin is never unregulated. After all, Bitcoin the protocol is ultimately a set of rules that regulate the decentralized digital currency (e.g. there will only ever be 21 million bitcoins), and the peer-to-peer network enforces these rules in its operation. Indeed, at its core, Bitcoin is an attempt at regulation through cryptography rather than human institutions.

But typically, when one hears that "Bitcoin is unregulated," the implication is that governments have not yet acted to "regulate" the digital currency in some way. This is incorrect because particular activities of actors employing the Bitcoin network are subject to any number of existing regulations. Even when the technology is not specifically mentioned in a law or regulation, an activity or use of a new technology can be covered by existing laws or regulation.

GUIDANCE VS. REGULATION

Regulations tend to be written broadly so that they can accommodate changes in the future. When a new technology like Bitcoin comes along, there are often questions about how exactly to comply with the existing regulations, but not necessarily questions about if the regulations apply. To address these how-not-if questions, regulators will issue guidance.

Guidance is not a new regulation, but a statement of how the existing regulation applies. The implication is that the regulation always applied to the new technology or activity, and that even without the guidance it would have applied. New regulations must first be proposed and regulators must consider comments from the public before promulgating a final rule. Guidance does not require due process because, technically, there is no new law being created; the existing applicable law is simply being explained.

For example, a business that accepts value from a customer and transmits it to a third party on behalf of that customer will be subject to federal money laundering and know-your-customer regulations, as well as state money transmission licensing requirements. The fact that Bitcoin is employed as the medium of exchange would not change the calculation. And this was as true in January of 2009, when Bitcoin first launched, as it is today.

In March of 2013, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued guidance explaining which actors in the digital currency space were covered by existing regulations and how they should comply.[13] FinCEN will tell you, however, that their guidance was not a new regulation, but a clarification of how their existing regulation already applied, and indeed applied from the inception of the Bitcoin network.[14]

Similarly, the Internal Revenue Service issued guidance on the tax treatment of capital gains from Bitcoin trading in March of 2014.[15] This did not mean that capital gains before the guidance were not subject to tax, but rather, the guidance explained how the tax that was already owed should be calculated. As far as the IRS is concerned, its regulations and the tax law always applied to Bitcoin traders with or without proffered guidance. Taxes on capital gains are due on trades as far back as January of 2009.

Often, however, an agency will not issue guidance and will simply enforce the existing law or regulation. If it is successful, it demonstrates that the law or regulation has always applied. The case of Trendon Shavers, the Texas man noted in the quote above, illustrates this.

Shavers was engaged in a Ponzi scheme in which he sold shares in a fund and promised investors returns of up to 1 percent per day, or 7 percent per week. When the Securities and Exchange Commission (SEC) brought suit against him, he argued that his fund offering did not qualify as a security under the law because "Bitcoin is not money, and is not part of anything regulated by the United States."[16]

The judge in the case found that, to the contrary, "It is clear that Bitcoin can be used as money." In a way, this now serves as guidance to all future actors

[13] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," FIN-2013-G001, March 2013, https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[14] FinCEN has also issued more comprehensive guidance on how their rules apply to crypto. *See:* "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," FIN-2019-G001, May 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

[15] Much of the IRS's guidance on several important sub-topics apart from the basic capital gains question has been insufficient or confusing; as such, legislation may now be needed to offer clarity. *See:* Landon Zinda, " If Budget Reconciliation is used for Tax Provisions, Crypto should be Included," *Coin Center,* December 18, 2024, https://www.coincenter.org/if-budget-reconciliation-is-used-for-tax-provisions-crypto-should-be-included/.

[16] *SEC v Trendon* T. Shavers, CASE NO. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013), https://casetext.com/case/sec-exch-commn-v-shavers-1.

who are considering issuing securities and taking investments in Bitcoin. And, subject to review by higher courts, of course, the precedent also means that this was always the meaning of the existing law; not that new law was created.

BITCOIN IS REGULATED

So, it's not right to say that Bitcoin is an unregulated digital currency given how many regulations apply to actors using the currency. And agency guidance underscores that fact. It's funny to see, then, that the articles quoted above were written well after FinCEN and the IRS had issued their guidance, and the judge in the Shavers case had issued his ruling.

Although there are important proceedings that will make new laws, like the New York Department of Financial Services BitLicense,[17] today, much of the public policy work to be done in the Bitcoin space is not developing new regulations. Instead, it's figuring out how existing regulations apply to activities that employ the Bitcoin network. Anyone who uses Bitcoin in a way covered by existing regulations is responsible for complying, and that compliance is not trivial. So let's be clear: for better or worse, Bitcoin is not unregulated.

TEN GENERAL PRINCIPLES FOR DRAFTING CRYPTO LEGISLATION

While much has been and can continue to be done to improve regulatory clarity through guidance, some policy issues are best solved with new law. The remainder of this guidebook will unpack ten general principles for drafting legislation. This is not a list of specific policy problems, nor is it a list of Coin Center's policy priorities. Instead, we have developed ten general principles, based on what we have observed in our history of working on crypto policy. These principles are intended to be helpful in drafting any legislation related to crypto no matter whether it is focused on consumer protection, market structure, crime-fighting or national security.

[17] Peter Van Valkenburgh, "What's in the Bitlicense's 5-year update?" *Coin Center,* June 24, 2020, https://www.coincenter.org/whats-in-the-bitlicenses-5-year-update/.

1. PROBLEM-FOCUSED RATHER THAN HOT-TOPIC DRIVEN

Legislation should be laser-focused at addressing a specific problem. Political realities and the media can sometimes pressure legislators to draft laws about a hot topic irrespective of a specific and well-articulated problem. Start with a real policy problem like a specific consumer risk, money laundering risk, or market inefficiency. Then identify why the new technology is changing the nature of the problem and which subcategory of "crypto" is relevant to the problem or its solution. Check if existing authority can address the problem and whether regulators have offered sufficient guidance on the topic. Only after that analysis should one ask whether and how new legislation can help solve the problem.

2. TECHNOLOGY-NEUTRAL RATHER THAN TECHNOLOGY-SPECIFIC

Once a particular problem has been identified, find the most technologically-neutral legislative solution. If the harm being addressed is, for example, money laundering, the law should target the problem generally and not create disparate standards for different types of technologies. For example, unless there is a significant difference in the way people launder money as between one technology versus another there is no reason to approach those technologies differently in anti-money-laundering legislation.

There are two fundamental reasons why laws should be technology-neutral: fairness and longevity. Unwarranted technological discrimination in legislation unfairly puts the government's finger on the scales between two technologies and can inappropriately benefit people or businesses that use or specialize in one of two competing technological solutions. If, for example, a corporation is highly invested in an existing technology that is made obsolete by new technologies, then they may lobby to unduly restrict that new technology and may do so quietly by insinuating that the reason for the new approach is some problem that in actuality exists irrespective of which technology is involved.

For example, in the wake of acts of terror or crime, some have called for specific regulation of cryptocurrencies for anti-money laundering purposes.[18] This happens despite the fact that far more money is laundered using traditional financial technologies than with cryptocurrencies,[19] and despite the fact that cryptocurrency intermediaries are already subject to the same anti-money laundering (AML) standards as traditional financial intermediaries.[20] Without a clear showing that either (a) the problem is worse in crypto, or (b) something about crypto is different leaving the existing laws insufficient, new technology-focused legislation may simply be anti-competitive or hot-topic motivated (see principle 1).

Additionally, technology-specific laws—even when justified—age poorly because of the rapid pace of technological change. For example, the Electronic Communications Privacy Act (ECPA) was passed in 1986 and unnecessarily differentiated between data stored in specific different formats.[21] Those distinctions made sense in a world when data lived on local hard disk drives and wasn't typically shared over the Internet, but they make no sense today in the world of cloud storage, email, and social media. Rather than taking a prescriptive approach to exactly what technologies should be subject to which controls, ECPA should have taken a technology-neutral principles-based approach focused on the privacy expectations of communicating persons, irrespective of which technologies they use to communicate.

There may be situations where technological change necessitates a new approach to a public policy question. However, this will often be the case not because a new technology has emerged and it needs regulating, but rather because a new technology has changed the risks and benefits involved in activities people have performed since long before that technology's emergence. While the technology warrants a new approach, the legislation

[18] Jesse Hamilton, "U.S. Treasury Debunks Narrative That Hamas Relied on Crypto to Fund Terrorism," *CoinDesk*, March 8, 2024, https://www.coindesk.com/policy/2024/02/14/us-treasury-backs-down-narrative-that-hamas-relied-on-crypto-to-fund-terrorism.
[19] "Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group," *Chainalysis*, February 15, 2024, https://www.chainalysis.com/blog/2024-crypto-money-laundering/.
[20] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," FIN-2013-G001, March 2013, https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.
[21] Electronic Communications Privacy Act (ECPA) of 1986, 100 Stat. 1848.

should still be focused on the activity and its risks rather than the technology itself.

3. ACTIVITIES-BASED AND RISK-CALIBRATED RATHER THAN TECHNOLOGY-BASED

People are subject to the law, not things. A law that obligates the ocean to stay clean is an obvious absurdity. Yet in the realm of technology, it can be less obvious when a thing rather than a person is the subject of some misguided law or regulation. As discussed earlier, when new technologies are a hot topic in the news or in politics, it can be tempting to draft legislation that is essentially targeted at the technology in the abstract rather than the specific activities performed by people using that technology.

Rather than having laws targeted at particular technologies, the law should enunciate principles for persons engaged in particular activities, such as entrusting data with another party, or safekeeping information or assets for a customer. These activities and the expectations of risk or benefit that they create in participants are effectively timeless even if the specific technologies involved change rapidly.

Technology may increase or decrease the risks or benefits of certain activities or broaden the class of people able to perform the activity safely, but our public policy concerns about the activity itself may not fundamentally change. For example, Bitcoin mining and Ethereum staking broadens the class of people who can validate financial transaction data from a handful of companies and associations (like SWIFT[22] or the credit card networks) to a larger set of persons: anyone with free software and sufficiently powerful consumer hardware. Mining and staking technologies also change the risks of performing that activity because digital signatures and blockchains make fraudulently manipulating transaction data infeasible.

Some technologies can significantly reduce the risks of an activity such that regulating that activity in the same way as before the technology existed would be absurd. For example, early elevators required a trained professional operator

[22] The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a Belgian banking cooperative that helps banks across the world settle over $150 trillion in financial transactions a year.

and regulations were developed to ensure that the operator was proficient in procedures for operating elevators and dealing with dangerous emergencies. With the advent of automatic door locks and braking systems, load sensors and call buttons, and the standardization of elevator controls it became absurd for regulations to continue mandating a human operator. Mining and staking activities are similar to the transaction message relaying and validation performed by traditional financial messaging organizations like SWIFT or Mastercard, but technological controls inherent in their operation make it absurd to regulate those activities as we regulated traditional intermediaries who had greater discretion and the ability to harm users of their system if they happened to be malicious or incompetent.

In these cases, it is critical to look at the risk engendered by the activity. Custodial banking service providers have full control and discretion over customer funds, and centralized financial messaging providers can fail to relay messages, effectively immobilizing funds even though they do not custody them, but a Bitcoin miner has neither custody nor blocking control over transactions.[23] We charter banks and regulate them for AML and prudential purposes. We regulate centralized financial messaging providers differently, subjecting them to some AML and countering the financing of terrorism (CFT) requirements but no prudential standards or licensing.[24] Finally, we should regulate miners and stakers differently, again, because they present neither the custody function of banks (an activity and risk that justifies prudential standards) nor the blocking ability of centralized financial messaging providers (an activity and risk that justifies some AML and CFT requirements).

[23] Peter Van Valkenburgh, "What is Bitcoin mining, and why is it necessary?," *Coin Center,* December 15, 2014, https://www.coincenter.org/education/advanced-topics/mining/.

[24] Despite facilitating the movement of trillions in bank transfers globally each year, SWIFT is not treated as a regulated financial institution under U.S. AML/CFT regulations. SWIFT has some certain obligations related to money laundering and terrorist financing, it is true, but these are obligations that have sprung from the creation of specific laws and treaties that explicitly identify SWIFT and solicit its participation in compliance efforts through mutual agreement. For example, Swift is subject to a US-EU treaty, the Terrorist Finance Tracking Program (TFTP). Under the TFTP, SWIFT has a specific obligation to comply with properly filed information requests from the U.S. Treasury, but this does not extend to performing AML/KYC checks or verifying the integrity of any transactional data or identities. This information sharing requirement is carefully specified in the TFTP, and SWIFT was included in the annex of that treaty as a "designated provider."

4. FOCUSED ON TRUSTED INTERMEDIARIES AND CONSCIENTIOUS OF DISINTERMEDIATION

Because only people are subject to the law, the obvious target for a regulatory obligation is the class of people or businesses who perform services for others as intermediaries. Intermediaries tend to be the least cost avoider, to borrow a term from law and economics. A least cost avoider is the party that can best minimize the costs associated with a particular harm. So if the harm in question is credit card fraud and the persons involved are merchants, customers, and the credit card networks, then the least cost avoider will probably be the credit card network. They have a top-down view of their entire payments network and can identify patterns of abuse and pause or reverse charges. Fraud can also be attacked by educating consumers and merchants so that scammers will have a harder time targeting them, but this will likely require more time and money for less reduction in fraud. The credit card network is the least cost avoider and, therefore, a good target for regulation.

Even though the ability to transact without intermediaries is the fundamental innovation behind cryptocurrencies, this doesn't mean the cryptocurrency ecosystem is without intermediaries. Most cryptocurrency users will continue to use a trusted third party to secure their assets and access trading services, just as most people do not keep all their cash in their home or make only non-intermediated cash transactions out in the world. Nor does the continued existence of trusted intermediaries defeat the point of cryptocurrency. Cryptocurrency is a great innovation because it provides an alternative to intermediaries when one is needed. If one is lucky enough to live in a place and time with stable governments and available financial service providers, there may not be much need for disintermediated payments technologies. But many in the developing world do not have those luxuries. Even in the developed world, one may want the option of disintermediated payments in case circumstances change and intermediaries become repressive, corrupt, or unreliable. In short, however, intermediaries aren't going anywhere, and for the vast majority of public policy problems—from investor protection to anti-money laundering—trusted cryptocurrency intermediaries remain the logical target for regulation.

Cryptocurrencies do, nonetheless, fundamentally change the scope of activities that an individual can perform without relying on a trusted intermediary if that individual wants to go it alone. A cryptocurrency user can hold her own crypto and send it across the world to a recipient without needing to rely on the good behavior or regulation of any person in between. Just because we once were able to regulate an intermediary who assisted people in performing a task does not mean we can or should regulate an individual who is performing the task for herself, nor does it mean we should regulate the person who created the technology that gives individuals the ability to do things themselves.

Cryptocurrency technologies are far from the first technology that radically broadened the class of people who can directly engage in an activity. As we just discussed, automatic elevator safety mechanisms allowed individuals to directly operate elevators rather than relying on a human operator. Ride-sharing apps like Uber and Lyft allowed users to directly hail a cab without the need to rely on a medallion system and human-operated dispatch service for safety and quality assurance. Self driving cars may soon allow even blind persons, children, or substantially disabled persons to travel alone by car to wherever they need to go.

Intermediaries aside, there are only two other potential targets for regulation: 1) people performing actions on their own accord, and 2) people who build and distribute tools that allow people to perform an action on their own. In both cases, regulation of these parities may be justified, but will need to be balanced against both the increased costs of regulating many individuals rather than a handful of intermediaries as well as the danger of trampling on fundamental rights.

To clarify with a metaphor, if the public policy problem we are looking at is residential building safety, there are only three possible targets of regulation: (1) professional home builders and designers, (2) residents and owners, and (3) tools and materials manufacturers. If most people hire a professional to build their home, then it makes sense to regulate professionals for design, methods, and materials standards. If more people start building their own homes, then similar regulations may be warranted, but will need to be balanced against certain fundamental rights like the liberty to do what one wants with one's own property and labor. If the thing that allows more people to build their own homes on their own is some new technology (e.g., 3D printing and design software), then the developers of those tools may be a justifiable target for regulation; however, these regulations must be balanced against still other fundamental rights, like the right of an inventor to publish her ideas (uphold free speech) and the right of an inventor to not be forced to publish ideas that are not her own (avoid compelled speech).

In the realm of tools and technologies, there is also the right of an individual to have access to tools that do not surreptitiously betray her privacy or agency. For example, we could require by law that all home security systems feed surveillance data to the police, and that all smart locks come with a back door so that a SWAT team can gain entry without a battering ram, but this would violate our fundamental right to privacy in our own homes.

We'll elaborate on how speech and privacy rights should be considered in cryptocurrency policymaking in the next two sections. To conclude this section, it is sufficient to identify three basic principles. First, cryptocurrency can enable disintermediation, but most people will continue to rely on trusted intermediaries for the majority of their cryptocurrency activities. Second, cryptocurrency intermediaries remain the least cost avoider and best target for regulations to address policy problems. Third, directly regulating the users of cryptocurrency tools or the designers of those tools should be a last-resort option for addressing grave public policy problems, and must always be balanced against the costs of regulating many more parties and the danger of trampling on fundamental rights.

5. FREE SPEECH-FRIENDLY

Cryptocurrency networks are powered by software. Software is a language for expressing ideas. It is speech, and whether software is published in a book, or on a website, or in a blockchain, it is protected under our Constitution from content-based prior restraints or compulsions. Sometimes, the new capabilities that cryptocurrency software makes possible can introduce new problems. Policymakers will then be driven to seek solutions. But in our American system, banning the publication of that software, stopping its distribution, or forcing the developers of that software to write it differently can never be considered a "solution." Americans are free to publish ideas, including software, without prior approval, and can never be made to publish ideas, including software, that are not their own or with which they fundamentally disagree.

In some ways, this is a broad prohibition on many potential forms of regulation and legislation. For example, many individuals and companies publish cryptocurrency wallet software. That software allows individuals to hold their own crypto and send it throughout the world, sometimes untraceably. Policymakers may prefer that wallet software include mechanisms to collect user information and report it to the government for either criminal or tax investigative purposes. Policymakers may prefer that wallet software include certain customer safety guarantees, like the ability to reverse a transaction within a discrete period of time after it is initiated or a particular form of disclosure about fees or other risks before the software processes any transactions for the user. These may be good or bad policies but, irrespective of their merit, they cannot be achieved by banning the publication of wallet software that does not include these features. Software developers cannot be forced to write software that includes these features. That approach is prior restraint and compelled speech, and it is not the way we regulate U.S. persons under our Constitutional system.

Further, many cryptocurrency tools also have so-called "front-end websites" where would-be users can quickly and easily engage with the underlying software using colorful graphic interfaces and helpful guides. Websites are also protected as speech, and developers should not be forced to license or get prior approval merely to publish and maintain a front-end website.[25]

An illustration can help outline the contours of this category. Critically, let's assume for now that the developer and maintainer of a front-end website does not exercise any discretion or control over what visitors do using the software found at that site. Let's also assume that there is nothing fraudulent about the software and website, the software does what the user interface suggests it will do and does not deceive the user into taking actions she did not intend to take. If the developer of this website merely publishes the software and interface to the internet where users use that software and connect to the underlying blockchain, then it would be unconstitutional to prohibit her from publishing that website in the first place (a content-based prior restraint on speech) and it would be unconstitutional to demand that she change aspects of the website or software to accomplish government objectives that she does not share (compelled speech).

[25] *303 Creative LLC v. Elenis*, 600 U.S. ___ (2023) (holding that under the First Amendment a plaintiff who created wedding websites could not be forced by state law to include in those websites speech in which she did not believe.).

While a free speech-friendly policy prescription may appear to be a massive limitation on any government regulation in this space, two important exceptions from First Amendment protection leave much room for reasonable and constitutional regulation: (1) expressive conduct, as compared with pure speech, gets lesser protections, and (2) false speech, such as fraud or defamation, gets no protection. These limitations become important when we weaken the assumptions we made in the previous paragraph: (A) our assumption that the developer does not have discretion or control over what visitors do using the software, and (B) our assumption that there is nothing fraudulent about the software.

If we have a developer who does exercise discretion or control—for example, they directly involve themselves with the user by learning about the user's unique circumstances and recommending a course of action to best address the user's needs (perhaps by offering investment advice or safekeeping assets)—then the developer is engaged in conduct rather than mere speech. Even though their conduct is mediated through speech, they can still, in many cases, be subject to regulations and controls without raising First Amendment difficulties.

For example, a lawyer does almost nothing but speak. Nonetheless, it is constitutional to demand that lawyers get a professional license in order to practice. It is also constitutional to hold lawyers liable for the unlicensed practice of law if they do not comply. If all that lawyers do is speak, how is this prior restraint constitutional? Because those laws target the conduct of the lawyer as he deals with his client, not his speech, they are constitutional. One can, in fact, give a general speech about the law to an audience without being a licensed attorney without being subsequently liable for the unlicensed practice of law. It's the agreement to speak on another person's behalf, to represent them in court, that is subject to licensing, not the speech that attends that conduct. The same should be true in crypto: the agreement to act on behalf of a customer should be regulated, not the software itself. But, without that agreement, there should be no regulation of software in the abstract.

In SEC v. Lowe, the Supreme Court articulated the divide between the regulation of professional conduct (which is generally constitutional) and that of speech (which is generally unconstitutional): It is constitutional to regulate a speaker who is "exercising judgment on behalf of [a] particular individual with whose circumstances he is directly acquainted," and the court calls that a “personal nexus” between speaker and audience.[26] By contrast, it is unconstitutional to regulate speech where the speaker has no such “personal nexus” with the intended listener. This is why regulating a custodial wallet and exchange would likely pass constitutional muster. Sure, the wallet and exchange tools are just front-end websites and back-end software and all of that is speech, but the software is mediating a personal nexus between the developer and the user: the developer is promising to safekeep the user’s cryptocurrency and the user is agreeing to the developer’s terms and paying any relevant fees for those services. By contrast, imagine a developer who has merely published wallet software at a website. When the user visits the site she can use the software to generate a cryptocurrency address and the associated cryptographic credentials to send cryptocurrency from that address and the resultant data is stored locally on the user’s computer. The developer never has discretion or control over what the user is doing with her software and website. While both examples involve a tool for safekeeping cryptocurrency and both involve protected speech, the latter example does not have the personal nexus inherent in the former. Without that personal nexus, it is unconstitutional to subject the publisher of that website to licensing or similar regulation.

If there is fraud involved, then the situation is even simpler. Say we have a developer who is actively deceiving the users of his software for personal gain by claiming that the software will do one thing while knowing full well that it will do something else. The developer has committed fraud and can be held fully liable for that criminal act even if all he did was publish software. Importantly, however, one can not permission all software publication contingent on a government auditor first checking for fraud. That sort of upfront censorship is a prior restraint on speech and is unconstitutional. Americans are free to publish potentially fraudulent, deceptive, and defamatory statements without review by a government censor, but they can absolutely be held liable for that conduct after the fact if a court finds that the statement was indeed false and harmful.

From a practical standpoint, how should a lawmaker approach constitutional limits in this space? First, lawmakers should target trusted intermediaries

[26] *Lowe v. SEC*, 472 U.S. 181 (1985), https://supreme.justia.com/cases/federal/us/472/181/.

rather than mere software or website publishers. These entities will almost certainly be engaged in conduct rather than mere speech and can therefore be licensed and compelled. Second, if one must target non-intermediaries, one should limit regulation to after-the-fact liability rules rather than preemptive licensing requirements. In practice, this looks like many of the regulatory regimes we have today. Investment advisors must register, but a person merely publishing a stock tip newsletter is not an investment advisor and cannot be forced to license.[27] Authorities can, however, still charge that publisher with fraud or unfair and deceptive acts and practices if it can be proved in court that his "hot tips" were indeed not so hot. Third, when drafting legislation targeting intermediaries in this space, take care to actually include and define the trusted activity that classifies someone as an intermediary. Mere facilitation of a transaction is not a trusted activity: Internet service providers facilitate online banking, but we would never require them to become chartered banks. Similarly, where possible, include explicit carve-outs from regulation for mere software and website development so as to ensure the law is not misapplied to regulate mere speech.

6. WITHOUT WARRANTLESS SEARCH AND SEIZURE

The Fourth Amendment, specifically its prohibition on warrantless search and seizure, is also highly relevant for drafting cryptocurrency legislation. Classical intermediaries who are in a position of trust vis-à-vis their customers have a reason to know their customers and to collect and retain records of those transactions. Once these trusted entities have this data, there are carve-outs to the Fourth Amendment's warrant requirement that apply: the trusted entities are legally considered "third parties" and under the "third party doctrine," the government can collect private information from these third parties without first seeking a warrant or other judicial review.[28]

As we've discussed, however, many participants in crypto are not trusted third parties: miners, stakers, software developers, and some front-end

[27] *Id.*

[28] *United States v. Miller,* 307 U.S. 174 (1939), https://supreme.justia.com/cases/federal/us/425/435/.

website maintainers. None of these parties have any reason to identify the users of their software or communications infrastructure; in fact, some may not even be able to if they wanted. None of these parties have reason to keep records of the activities of those users. Users have no customer agreements or privacy agreements with those entities. Because of all this, the third party doctrine does not apply. Users have not voluntarily provided their private information to a third party for a legitimate business purpose. According to Supreme Court precedent it would, therefore, be unconstitutional for thegovernment to demand private identification or transaction information from these parties without a warrant.[29]

From a practical standpoint, lawmakers drafting legislation should be mindful of whether they are seeking warrantless data collection from a truly trusted intermediary, in which case the collection may be constitutional under the third party doctrine, or whether they are attempting to force the collection of private data from individual users or non-intermediating software developers, in which case the collection is likely an unconstitutional warrantless search and seizure. Legislation should always require a warrant before that data is collected. The Constitution doesn't prohibit surveillance outright, it simply says that direct surveillance of an American's home or person should always be checked and limited by a warrant requirement.

7. WITHOUT LEGISLATIVE DELEGATION

Regulating activities performed using new technologies is, by nature, highly technical. Accordingly, there is an impulse to hand discretion to the executive branch rather than spell out the nature of the regulation in legislation. The Constitution, however, vests all legislative power exclusively in the hands of Congress.[30] It is constitutional to delegate some power to the Executive in legislation. For example, if Congress wishes to

[29] *United States v. Miller,* 425 U.S. 435 (1976); *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

[30] U.S. Const. art. I, § 1. For a general overview of the non-delegation doctrine's application to crypto, see Peter Van Valkenburgh, "Broad, Ambiguous, or Delegated: Constitutional Infirmities of the Bank Secrecy Act," *Coin Center,* November 2023, https://www.coincenter.org/broad-ambiguous-or-delegated-constitutional-infirmities-of-the-bank-secrecy-act/.

create a licensing regime for crypto businesses, it can leave many details of that regime to the regulator. It could identify a general principle in law, for example, "adequate background information on the licensed party to prevent fraud may be demanded" or "licensed parties shall maintain adequate capitalization to prevent liquidity and guard against contagion risk." The regulator can take these principles and fill in the details, deciding exactly what level of information collection and capitalization is adequate to ensure the explicit statutory purpose is achieved.

It is, however, not constitutional to allow the regulator full discretion in whether to apply the law, or to determine the category of persons to whom the law is going to apply. For example, the law should not leave definitional questions to the regulator such as, "the regulator may, through rulemaking, determine who is a financial institution required to license under this chapter" or "the regulator may, through rulemaking, determine what activities trigger a licensing requirement." By giving the regulator discretion to apply a licensing requirement to whoever they want, Congress would be delegating its exclusive legislative power to the executive in contravention of our Constitutional system.[31]

8. WITHOUT EXCESS AMBIGUITY OR BREADTH

Nor should a lawmaker leave too much in the law ambiguous and up for regulatory interpretation. Definitions of regulated parties and regulatory obligations should be sufficiently definite that a reasonable person can interpret the plain meaning of the text and understand who is obligated and what those obligations require. In Loper Bright Enterprises v. Raimondo, the Supreme Court ruled that the regulator will not get deference for their interpretation of an underlying law.[32] If the court believes that the plain meaning of a law differs from the regulator's interpretation, the plain meaning will control.

Nor should a lawmaker seek to regulate an exceedingly broad class of activities. For example, the Supreme Court has found that a law prohibiting two or more persons from congregating in public if any of them are convicted felons is excessively broad; it could, for example, make it a crime for a father and son to watch a baseball game. The legislation was, of course, not aimed at stopping

[31] *Id.*

[32] *Loper Bright Enterprises v. Raimondo*, 144 S. Ct. 2244, https://www.supremecourt.gov/opinions/23pdf/22-451_7m58.pdf.

father-son outings; it aimed at breaking up criminal gang meetings. It was, therefore, too broad in its drafting.[33]

Excess legislative breadth is often confused with excess ambiguity because both ills often result in a similar problem: the average citizen is not able to understand when the law will apply to her activities.[34] An ambiguous law leaves the citizen unsure whether her course of conduct is the type of conduct prohibited. A broad law may be clear about what conduct is prohibited but, because so much conduct is theoretically prohibited, an average citizen must guess whether the police will actually actively pursue her activities rather than someone else.

This is particularly relevant in crypto legislation because technology has now enabled far more people to engage in an activity previously reserved for a select few. If we treated every person who now facilitates financial transactions as a licensed financial institution, we would be subjecting tens of thousands of Americans who use free software and an Internet connection to mine, stake, or relay cryptocurrency messages to an invasive and costly regulatory regime. If it is infeasible to demand that of everyone, it is fundamentally unfair to impose an obligation that will be enforced only sporadically. Worse, exceedingly broad laws afford the government excess discretion to pick and choose targets. Law enforcement may charge a person with a broad law because of political or personal reasons rather than because they are fairly enforcing the law against all who violate it.

Ultimately, excessively ambiguous or broad laws create constitutional due process problems. If a reasonable person cannot read the law and generally understand whether it obligates her to change her course of conduct, then it is unconstitutional to hold that person liable for violations of that law. Under the Fifth Amendment, the law can and should be struck down as unconstitutional.

[33] *Chicago v. Morales,* 527 U.S. 41 (1999), https://supreme.justia.com/cases/federal/us/527/41/.

[34] Peter Van Valkenburgh, "Broad, Ambiguous, or Delegated: Constitutional Infirmities of the Bank Secrecy Act," *Coin Center,* November 2023, https://www.coincenter.org/broad-ambiguous-or-delegated-constitutional-infirmities-of-the-bank-secrecy-act/; Kiel Brennan-Marquez, "Extremely Broad Laws," (2019). Faculty Articles and Papers. 589. https://digitalcommons.lib.uconn.edu/law_papers/589/.

9. WITH PROCEDURAL DUE PROCESS

The Fifth Amendment also guarantees our right, as Americans, to a fair and impartial trial, access to legal representation, the ability to present evidence and witnesses in one's defense, the right to appeal a decision, and the protection against self-incrimination, essentially ensuring that no one can be deprived of "life, liberty, or property, without due process of law."[35] As with any legislation, cryptocurrency legislation that threatens or imposes penalties must provide these due process protections to pass constitutional muster. Laws that, for example, allow the regulator to determine one's guilt for non-compliance without any recourse for an appeal to an Article III court would not be constitutional.

Some financial regulatory rules exist in a grey area with regard to procedural due process. For example, the special measures provision of the PATRIOT Act allows the Treasury to engage in rulemaking to ban financial institutions from processing transactions of a certain type.[36] The constitutionality of this provision has yet to be adjudicated. If, for example, an administration were to use its special measures powers to order regulated financial institutions to ban all transactions related to cryptocurrency, a substantial liberty interest of many Americans would be decidedly curtailed without any trial or opportunity for review. The notice and comment requirements of the special measures powers provide some opportunity for public review, but no court has yet found that they can substitute for long-established procedural due process rights. Within the last five years, bills have occasionally been introduced that would have removed even the notice and comment process from the special measures power. That entirely unchecked power to restrict the liberty of American citizens would almost certainly be unconstitutional under the Fifth Amendment. Wherever possible, legislators should include the usual procedural safeguards to ensure constitutionality and honor the rights of Americans.

[35] U.S. Const. amend. V.

[36] 31 U.S.C. § 5318A

10. WITH A REQUIRED FOREIGN NEXUS FOR ANYTHING NOT MEETING CONSTITUTIONAL MUSTER

The previous five sections on constitutional law create a strict set of limitations on Congress's ability to legislate. Some constitutional provisions, however, apply less strictly in the context of foreign persons. For example, sanctions laws can carry extraordinary penalties for those who are identified as sanctioned persons.[37] Once sanctioned, a target can expect to lose all banking relationships and become unable to transact with any American persons. All of this happens without any indictment, trial, ruling, or appeal process; one simply finds that one's name has appeared on the list of sanctioned persons.[38] To the extent that sanctions laws are constitutional at all, it is because they can only be used to sanction non-Americans, for whom some constitutional due process protections may not apply. In extraordinary circumstances where national security demands an aggressive approach to terrorism and crime, some law and policy may eschew the normal procedural and constitutional limitations if and only if the law is explicitly drafted to carve-out U.S. persons who enjoy the full protection of our Bill of Rights.

[37] 50 U.S.C. § 1702 et seq

[38] *See:* U.S. Dep't of Treasury, Specially Designated Nationals and Blocked Persons List (SDN) Search, https://sanctionssearch.ofac.treas.gov/.

CONCLUSION

Developing effective cryptocurrency policy is one of the most challenging endeavors one can take on in Washington. Coin Center's mission is to make that challenge a little bit easier with education and research. It's also Coin Center's mission to defend the rights of individuals to build and use free and open cryptocurrency networks. By following the ten principles we've explained throughout this guide, we hope you can achieve your policy goals while preserving the freedom to innovate.

For 10 years Coin Center has dedicated itself to being a resource for staff and members grappling with these important and complex issues. We hope this guide will conveniently distill some important lessons we've learned over that period. We also hope our help will not end here; we are always available as you work at the exciting intersection of law and technology. Please do not hesitate to reach out for a member briefing, a quick chat, or anything in between.

COIN CENTER

coincenter.org