TESTIMONY OF

Jason Somensatto
Director of Policy, Coin Center

BEFORE THE

United States House of Representatives Committee on Financial Services
Digital Assets, Financial Technology, and Artificial Intelligence Subcommittee

Building the Future of Finance: How the CLARITY Act Unlocks Innovation

July 17, 2026

One year ago, in an overwhelmingly bipartisan vote, the House passed the Digital Asset Market Clarity Act (CLARITY). Through CLARITY, the House navigated the difficult task of empowering the market regulators to implement a robust and comprehensive regulatory framework, providing centralized intermediaries and market participants with clarity around the regulatory obligations and protections that will apply in this emerging market, and promoting the underlying innovation of blockchain networks by protecting developers from unnecessary regulation.

As the Senate works to put the final touches on its version of CLARITY, this hearing provides a valuable opportunity to zoom out and discuss why this legislation is so important to pass. At a high level, crypto market structure legislation must both create clear rules for centralized intermediaries and protect the open, peer-to-peer architecture that makes decentralized blockchain networks meaningfully different from traditional financial infrastructure.

Coin Center has long supported these goals and has been calling for such legislation since 2018.

Coin Center is an independent research and advocacy organization focused on the public policy issues raised by cryptocurrency and decentralized computing technologies such as Bitcoin and Ethereum. We do not represent any exchange, issuer, asset manager, or other business that may benefit from or be affected by the CLARITY Act. Rather, we are mission-focused on the broader public interest in open blockchain networks, software development, self-custody, peer-to-peer transactions, and the civil liberties that these technologies can protect.

Blockchain networks are not merely a new way to trade assets. At their best, they are open computing networks that allow individuals to hold and transfer value without depending on a bank, exchange, payment processor, or other centralized intermediary. They allow developers to freely build interoperable tools on shared infrastructure. Indeed, this is the fundamental purpose of blockchains—to give individuals the freedom to transact in a peer-to-peer manner without being censored or unnecessarily surveilled and to give developers the freedom to innovate novel infrastructure that does not require permission to build.

For that reason, Congress should be careful to distinguish between the underlying technology of blockchain networks and the industry of businesses that leverage that technology to serve customers. The CLARITY Act appropriately recognizes that distinction by establishing a comprehensive regulatory framework for businesses that present traditional market and consumer risks, while ensuring that those who develop and support the underlying technology can continue innovating without being subject to inappropriate regulation.

I. Why Federal Market Structure Legislation Is Needed

Coin Center has long supported the creation of a federal regulatory framework for cryptocurrency markets. In 2018, we published a report calling for a federal alternative to state-by-state money transmission licensing for cryptocurrency exchanges and other custodial intermediaries.[1] That position was based on the view that national and global markets should not be governed primarily by a patchwork of state licensing regimes designed for a different era and type of financial activity.

Cryptocurrency markets have developed in some ways that are familiar to financial regulators. Centralized platforms custody customer assets, facilitate trading, provide market access, and serve as important gateways between traditional financial infrastructure and blockchain networks. These businesses can present custody risk, conflicts of interest, fraud, manipulation, inadequate disclosures, and failures of market integrity, all of which are the kinds of risks that market regulation is designed to address.

A clear federal regime can identify those risks, assign responsibility to the right actors, and give regulators the authority they need to supervise the market. It can also give responsible

[1] *See* Peter Van Valkenburgh, *The Need for a Federal Alternative to State Money Transmission Licensing*, Coin Center (Jan. 2018), https://coincenter.org/the-need-for-a-federal-alternative-to-state-money-transmission-licensing/.

businesses a path to compliance, rather than forcing them to navigate overlapping and sometimes inconsistent regulatory theories. Ultimately, regulatory clarity means the imposition of rules that identify who is responsible for what, which risks they create, and which regulator has authority to supervise those risks.

The current state of law is not serving consumers, developers, entrepreneurs, or regulators well. Some agencies have attempted to stretch existing authorities to reach conduct that does not fit comfortably within old categories. States have continued to rely on money transmission laws that vary across jurisdictions and were not designed to function as a comprehensive national market structure regime. Meanwhile, serious actors face uncertainty, and less serious actors can exploit confusion.

Federal legislation is the appropriate response. Congress should decide how cryptocurrency markets are regulated. It should decide which intermediaries must register, which regulator has jurisdiction, what standards apply, and what protections are owed to customers.

II. Empowering the CFTC to Ensure Market Integrity

Fortunately, the CLARITY Act would accomplish that goal. It gives federal regulators clearer authority over centralized, custodial markets and intermediaries. It creates a path for lawful cryptocurrency activity in the United States. And, critically, it does so without forcing all activity on blockchain networks into the mold of centralized financial intermediation.

As an alumnus of the Commodity Futures Trading Commission, I spent several years analyzing what type of authority and resources the CFTC would need to ensure that cryptocurrency markets could meet the gold standard of U.S. regulated markets. At a basic level, that requires three things. First, the CFTC needs authority to define and register the centralized exchanges, brokers, and dealers that intermediate spot crypto commodity markets. Second, those registered entities must be subject to core standards addressing customer asset protection, conflicts of interest, trading integrity, operational resilience, capital, recordkeeping, and anti-money laundering obligations. Third, the CFTC must have the ability to surveil these markets, obtain information from registered entities, police manipulation and fraud, and enforce the rules against firms that operate outside the framework. CLARITY appropriately addresses each of these elements.

Just as important, however, a market structure bill must define the limits of that framework. Clear registration categories help regulators oversee real intermediaries, but they also help prevent regulators from treating every developer, validator, wallet provider, or interface as though they were operating a financial marketplace. The same clarity that tells centralized businesses when they must register should also tell non-controlling developers when they are not acting as regulated intermediaries.

III. Developer Protections Are Essential to Preserving Open Blockchain Networks

The central policy challenge in cryptocurrency legislation is drawing the line between intermediaries and technology. CLARITY is important because it largely draws that line in the right place.

A workable framework must distinguish between a business that takes custody of customer assets and a developer who writes software that users may run for themselves. It must distinguish between an exchange that matches trades for customers and a person who publishes neutral code. It must distinguish between an intermediary that can move, freeze, or misuse customer funds and a toolmaker who never controls those funds in the first place.

This distinction may sound, at first, like a special exemption for blockchain developers. It is not. The same line between regulated intermediaries and unregulated toolmakers exists across industries and technologies. Traditional banking offers a simple example. We regulate banks because they hold themselves out as trusted custodians of other people's money. A bank that takes deposits, manages customer accounts, and promises to safeguard customer funds should meet rules designed for that role. Indeed, a person should be forbidden from taking customer deposits if they cannot, or will not, comply with rules designed to protect those customers.

But we do not require every locksmith, vault designer, alarm engineer, website developer, cryptographer, or architect to obtain a banking license before building better tools for securing property. The law regulates the institution that assumes a position of trust over customer assets; it does not pre-approve every scientist, engineer, or software developer whose work may improve the technologies that banks and individuals use.

Such a pre-approval regime, when applied to innovators who publish and share their inventions, would be hostile to technological progress and in deep tension with our constitutional tradition of protecting speech, publication, scientific inquiry, and useful innovation.[2]

[2] *See* Peter Van Valkenburgh, *Software is Speech: Why Regulators Cannot Invent the Missing Middlemen*, Coin Center (Apr. 2026), https://coincenter.org/software-is-speech-why-regulators-cannot-invent-the-missing-middlemen/.

The same distinction matters for open blockchain networks. A centralized exchange or broker that takes custody of customer assets can properly be regulated as a financial intermediary. But a developer who writes non-custodial wallet software, publishes open-source code, validates transactions, or builds infrastructure for a decentralized network is not holding customer funds or standing between a customer and the market. Treating that developer like a financial intermediary would be like requiring a vault engineer to get a bank charter before designing a stronger safe.

This distinction is especially important because many activities by developers in the blockchain ecosystem are not the types of activities that should trigger regulation. A blockchain developer may publish code that anyone in the world can inspect, copy, improve, or run. A security researcher may identify vulnerabilities and propose patches. A wallet developer may create software that helps users hold their own assets. A node developer may help maintain software that allows a network to function. These activities are not the same as operating an exchange, acting as a broker, taking custody of customer funds, or transmitting money on behalf of another person.

As a result, developer protections are key to market structure legislation.[3] If Congress creates clear rules for centralized cryptocurrency businesses but leaves developers exposed to open-ended liability for building non-custodial software, then the legislation will have protected part of the market while undermining the technology that makes the market possible.

This is not only about protecting developers as a class. It is about preserving the values that make open blockchain networks worth protecting in the first place.[4] These networks allow individuals to hold assets directly, transact without platform permission, and use software that is inspectable, interoperable, and resistant to centralized control. Those features support privacy, competition, open access, and individual autonomy. They also reflect long-standing American commitments to free expression, technological experimentation, and permissionless innovation.

---

[3] *See* Peter Van Valkenburgh, *Senate market structure negotiations must not sacrifice hard won developer protections*, Coin Center (Nov. 6, 2025), https://coincenter.org/senate-market-structure-negotiations-must-not-sacrifice-hard-won-developer-protections/.

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

A. CLARITY protects developers from being misclassified as SEC and CFTC-registered intermediaries

The CLARITY Act recognizes these principles in several ways. It includes protections designed to ensure that software developers and infrastructure providers are not required to register with the SEC or CFTC simply because they write code, publish software, validate transactions, maintain a protocol, provide a user interface, or otherwise support the functioning of a blockchain network without taking control of customer assets or acting in a trusted capacity as a traditional intermediary.

A person who writes non-custodial wallet software is not performing the same function as an exchange that holds customer assets and matches customer trades. A developer who contributes code to a decentralized protocol is not acting as a broker or dealer. A miner, validator, or node operator who maintains network infrastructure has no customers and is not taking custody or control of customer funds. Regulation should turn on role, relationship, custody, control, and agency. It should not turn on whether software is useful.

It is worth noting that CLARITY carefully draws this line between regulation and developer protection without undermining existing regulatory protections. The full range of securities laws still apply to those who meet the existing definitions of SEC registered intermediaries. Likewise, new intermediary categories have been defined to capture businesses to be regulated in the digital commodity market without impacting existing derivatives law regulation. For those appropriately subject to registration requirements, the Bank Secrecy Act still applies, ensuring that they implement anti-money laundering programs that help prevent illicit activity. In other words, CLARITY's developer protections do not create a regulatory loophole for financial intermediaries. They simply ensure that regulation remains focused on those who actually perform intermediary functions.

B. The BRCA addresses the most serious threat to non-controlling developers

The CLARITY Act similarly protects developers through the Blockchain Regulatory Certainty Act. The BRCA addresses the most serious risk facing non-custodial software developers: being treated as unlicensed money transmitters even though they never take control of customer funds.

Money transmission laws are premised on an intermediary accepting and transmitting money on behalf of another person. The reason money transmitters are regulated is that they stand between the sender and recipient. They take control of money. They can lose it, steal it, delay it, redirect it, or use it for unlawful purposes. Regulation attaches to that position of trust and control.

Non-custodial software development is different. Publishing code is not equivalent to accepting and transmitting money, and a person who lacks the unilateral ability to control, initiate, or effectuate transactions involving user assets should not face money transmission liability merely because others use software they wrote. This important distinction has been recognized by FinCEN in its 2019 guidance, which differentiated between those businesses that must register as money transmitters and implement an anti-money laundering program based on whether they had "total independent control" of a customer's assets.[5]

The BRCA puts this important principle into statute so that prosecutors and regulators cannot simply reinterpret the law in an effort to hold developers liable for criminal actions they have no control over. This risk is not hypothetical. In recent years, aggressive interpretations of money transmission law have created real uncertainty for developers of non-custodial blockchain tools. Indeed, the Department of Justice has pursued multiple cases based almost exclusively on the theory that non-controlling developers should be held criminally responsible for illicit transactions made by others using their freely available software rather than proving more substantive money laundering charges.[6]

The BRCA does not mean bad actors are beyond the reach of law enforcement. Fraud and theft remain illegal. Sanctions evasion, money laundering, conspiracy, and aiding and abetting remain illegal. Custodial businesses that accept and transmit customer funds remain subject to applicable licensing and anti-money laundering obligations. The BRCA does not create a loophole for regulated businesses to avoid obligations that apply for independent reasons. It merely removes the threat of aggressive and unfounded overreach by regulators and prosecutors.

That threat chills innovation from honest Americans. It does not merely deter bad actors. It deters responsible developers, open-source contributors, security researchers, wallet builders, and infrastructure providers from building in the United States. A vague threat of criminal liability is especially damaging in an open-source ecosystem, where innovation often comes from individuals and small teams rather than large institutions with compliance departments and outside counsel.

Preserving the BRCA is therefore essential to preserving the broader architecture of CLARITY. The bill should create a federal framework for businesses that perform financial intermediary

---

[5] FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FinCEN Guidance FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[6] *See* Peter Van Valkenburgh, *DOJ's New Stance on Crypto Wallets is a Threat to Liberty and the Rule of Law*, Coin Center (Apr. 29, 2024), https://coincenter.org/dojs-new-stance-on-crypto-wallets-is-a-threat-to-liberty-and-the-rule-of-law/.

functions. It should not expose developers to criminal liability for declining to become intermediaries in the first place.

These developers are worth protecting because they embody American values and advance American interests abroad. They build and release open public infrastructure that anyone in the world can use without permission, intermediation, or centralized control. That infrastructure is a public good because it gives individuals a means to preserve their privacy, exercise autonomy, and participate freely in markets and political discourse. It is especially important in a world where governments and private platforms increasingly exert their power to monitor, restrict, or control access to financial infrastructure.

IV. Conclusion

Congress does not need to choose between market regulation and open innovation. The task is to regulate the intermediaries that create custodial and market risks while preserving the open, peer-to-peer architecture that makes blockchain networks valuable.

The CLARITY Act does that. It provides a path toward federal oversight of centralized cryptocurrency markets, while protecting developers, self-custody, and peer-to-peer use. For that reason, Coin Center supports the continued advancement of the CLARITY Act and urges Congress to enact market structure legislation into law.