Polygon Labs is a software development company that builds open, permissionless blockchain infrastructure solutions and complementary software, including zk-enabled technology, to make mass adoption of a blockchain-based Internet a reality. We define success as a blockchain-enabled Internet open and useful to billions across the globe. In addition to creating accessible, secure technology, we believe that education about blockchain and advocacy for sound laws are significant parts of achieving this vision.

Coupled with the technology, the Polygon community is critical in helping achieve the vision of web3 mass adoption. To create a collaborative and constructive environment for addressing web3 policy, we owe it to you to let you know where we stand and give you an opportunity to tell us your views. At the same time, we want to respect the desire of policymakers and their staff to make decisions in private until they have decided to share work with the public.

Below we outline four core principles that will guide our approach to laws and regulations around the world for web3 technology (*e.g.*, base layers, scaling infrastructure, decentralized applications, interfaces, wallets). We are committed to collaborating with stakeholders throughout the web3 ecosystem and want to hear from you: reach out to our Policy team at policy@polygon.technology.

Core Policy Principles

1. Software development should be protected to ensure continued innovation.

Developing software is not a regulated activity today. Only those who offer the developed software to customers are subject to consumer protection and other relevant laws.

This framework should apply equally to the development of blockchain and blockchain-based software. As has been recognized in the historical approach to regulating technology development, imposing laws directed at software development will chill innovation and ignore the opportunities of an Internet that users, rather than Big Tech, control.

We will oppose proposed laws and legislation that seek to regulate software developers for the writing and publishing of code. In addition, we will oppose regulation that will turn software developers into centralized intermediaries simply for writing code or creating protocols.

2. Decentralization is different: regulatory objectives present in the traditional, centralized world can be achieved through laws that address the realities of decentralized protocols.

Decentralization – the North Star of blockchain technology – creates new systems and paradigms: rather than one intermediary sustaining the system, hundreds or thousands of independent contributors do. Given the lack of intermediaries needed in blockchain networks and applications, laws and regulations that apply to old, centralized systems run by intermediaries will not work for decentralized software services.

The ideal of "same risk, same regulation" – as cited by regulators – must be properly tailored to decentralized, blockchain-based systems. We acknowledge that blockchains and related technology built on and around them pose various risks. However, in ***true*** decentralized, blockchain-based systems, risks do not arise in the same way as in traditional systems (*e.g.*, risks may arise through vulnerabilities in code without human involvement), and thus, the "same regulation" cannot apply in the "same way". In addition, it must be recognized that we can leverage certain functions of blockchain-based systems to address regulatory goals (*e.g.*, peer-to-protocol transactions eliminate counterparty risk and increase certainty, but also raise new risks as noted above).

Protecting users, preserving market integrity and combating illicit finance – core regulatory objectives – ***can*** be achieved in a decentralized, permissionless system, but must be done differently than in traditional systems. Simultaneously, protecting the integrity of decentralized blockchain-based technology will ensure that the technology has the opportunity to achieve the full extent of its promise, namely, providing access to those who were previously excluded from the global economy and empowering self-ownership and self-custody.

We will advocate for novel and web3-native solutions to legal and regulatory issues in decentralized, blockchain-based systems to address lawmakers' objectives.

We are also committed to educating policymakers on how to identify decentralization as well as how to protect the integrity of decentralized systems and their users.

3. *Regulate activities; be technology neutral.*

Today, laws regulate activities undertaken by entities or individuals. Centralized actors providing particular services must abide by laws that apply to those services. Such laws are needed to allow consumers to "trust" intermediaries: the people and entities that have control over their systems and their customer's assets and data and are trusted to act with care.

The same must hold true for any laws that relate to blockchain technology and the web3 ecosystem; laws need to address *activities* rather than the technology itself. Where individuals or entities in the web3 world perform the same roles as or provide services similar to traditional intermediaries, they may be subject to similar laws, adjusted as needed to accommodate benefits and address respective risks. However, where technology replaces functions typically performed by persons in traditional systems, lawmakers should not import or otherwise force the existence of intermediaries to which to apply traditional regulation.

Regulation should remain unbiased against technology, and laws should respect that blockchain-based software can allow individuals to be stewards over their own personal data.

Any laws that address activities rather than technology alone will be evergreen and grow with the technology.

4. *Security and transparency are key to user protection.*

User protection is paramount in ensuring full and fair functioning of decentralized, blockchain-based Internet systems. (We intentionally use the term "user" rather than "consumer" or "investor" because there is no privity in this type of system; there are only those who engage with the software on their own terms.) Blockchain technology and decentralized applications must be created and deployed with the safety of users in mind. This objective can be met – as an initial matter – in two ways.

First, technology-enabled security of blockchain networks and decentralized applications built on them ensures that blockchain-based technology can be used safely without needing to trust a centralized intermediary. The more immutable, censorship-resistant and secure a blockchain protocol or application, the more users will be able to rely on the integrity of the entire system. In the world of decentralized blockchain-based software, security of a network or protocol is a critical step to "user protection."

Second, in line with the web3 ethos, transparency is fundamental and, in the regulatory context, has two primary components: (i) disclosures by developers and stakeholders as it relates to certain activities; and (ii) source available code.

As to the former, all disclosures should be complete, straightforward and understandable by any user – and should avoid technical jargon. This will protect users by bringing information already on blockchains to a place users can easily find and understand it, making them more secure in using such software. Full and fair disclosure will increase accountability for all participants in the blockchain space.

As to the latter, when users know the code is fully available for review – even if they themselves cannot read or audit the code – there is an additional layer of security because that demonstrates both that anyone can audit and ensure the safety of the code and that someone could identify whether there are hidden aspects of centralization.

These ideals of transparency remain consistent with the privacy that novel applications of blockchain technology, such as zk-proofs, afford users – deciding when and how to self-custody their information.

With the benefits of security and transparency will come increased adoption and growth of the web3 ecosystem.