COIN CENTER

May 15, 2017

Mr. Dinesh Sharma
Special Secretary (Economic Affairs)
Department of Economic Affairs
Ministry of Finance
Government of India
New Delhi, India - 110001

Dear Sir,

We understand that a committee under your chairmanship is conducting a review of the proper regulatory framework for cryptocurrencies such as Bitcoin. Coin Center is the leading non-profit research and advocacy center focused on the public policy issues facing cryptocurrency and decentralized computing technologies like Bitcoin and blockchain technology. It is an independent organization based in Washington, D.C., U.S.A. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

Over the past three years we have developed a large body of policy thinking in this area and have consulted with many government bodies and have provided expert testimony to several U.S. states, the U.S. federal Congress, and to the European Parliament. All of our work is available publicly on our website at coincenter.org.

We are writing to you to let you know that we are available to you as an expert resource as you consider these issues. We would welcome the opportunity to answer any questions you may have and to discuss the approaches that various U.S. and international jurisdictions have taken. To that end, we would like to share with you six principles that we have found to be at the heart of successful approaches to government regulation or self-regulation by the industry:

1. Understanding who and what can be the subject of regulation

Like the Internet, the network of computers that power a cryptocurrency is decentralized. There are thousands of individuals and businesses all around the world that run the cryptocurrency software on computers that they own and maintain independently. Together all of these computers form the network and provide throughput for transactions on that network. This means that, like the Internet, there is no way to regulate the network or the system itself as a whole. It may be possible to regulate individual parties who use the network (*e.g.* a

customer-facing business that safekeeps bitcoins for their users), but the network as a whole is a decentralized web not amenable to easy regulation.

2. Clearly articulating the goals of a cryptocurrency regulatory policy

Cryptocurrency regulatory policy should have clearly defined goals. In general there are two primary goals: consumer protection and engaging in anti-money laundering. The goal of a consumer protection regulation should be to ensure that whenever a company *holds cryptocurrency on behalf of their customer* that they have policies and practices in place to ensure that the customer will not lose their cryptocurrency either because the company went bankrupt, got hacked, failed to have insurance, or otherwise mismanaged the cryptocurrency with which they were entrusted. The goal of an anti-money-laundering regulation is to ensure that businesses holding and transmitting cryptocurrency on behalf of their customers keep adequate records of customer identification and report suspicious activity to the regulator when appropriate.

3. Only regulating persons with "control" over consumers' cryptocurrency

In the U.S., traditional financial regulation for consumer protective or anti-money-laundering purposes focuses on custodial intermediaries. We require a bank charter or money transmission license from a company that holds other people's valuables on their behalf, but not from a company that builds safes, armored cars, leather wallets, or any other product that allows persons to secure and safekeep their own valuables on their own behalf.

In the cryptocurrency space it can be difficult to determine which actors are playing the role of a custodial intermediary and which are performing other non-custodial activities. The companies and individuals performing non-custodial activities are essential to innovation. They are the persons that help build the fundamental network and software infrastructure that allow these technologies to grow and flourish. In order to be clear that only custodial intermediaries are required to be regulated parties, laws and regulations should, wherever possible, clearly define the act of *controlling* cryptocurrency on behalf of another person.

In the U.S., the Uniform Law Commission has pioneered an excellent and easy to administer definition of control:

> "the power to execute unilaterally or prevent indefinitely a [cryptocurrency] transaction"[1]

In a national law regulating cryptocurrency intermediaries, this definition of control should be given, and then the scope of regulation should be explicitly *limited to persons who in the regular course of business have control over the cryptocurrency of a consumer.*

4. Cooperating with businesses to preserve visibility

[1] *See* ULC *Regulation of Virtual Currency Businesses Act*, *available at* http://www.uniformlaws.org/Committee.aspx?title=Regulation%20of%20Virtual%20Currency%20Businesses%20Act.

When it comes to anti-money-laundering policy, it is important to work with companies in the space rather than against them. Like the Internet, or encryption technology, cryptocurrency networks will exist and operate regardless of any government policy, and there will likely always be businesses or individuals ready and willing to help people convert local currency into various cryptocurrencies. By offering a reasonable path to regulation for exchangers, however, regulators can obtain windows into these networks.

The exchanger, like any other financial intermediary in a position of trust, can collect information about their customers and take a risk-based approach to detecting money laundering or illicit financing activities. In the U.S., for example, all major exchanges are registered with FinCEN, the division of the U.S. Department of Treasury that specializes in anti-money-laundering regulation. If there is no reasonable path to becoming a regulated exchange in a given country, then these windows close, and law enforcement is left with less information about illicit activities. The country's citizens will likely still be able to access exchanges based in other countries, who may not choose to be compliant or helpful with regard to providing information to regulators.

5. Treating all cryptocurrencies equally

In the U.S., regulators have wisely drawn no distinction between one cryptocurrency versus another. There is no system in place for determining which cryptocurrencies can or cannot be used by regulated businesses, and all cryptocurrencies are treated identically under the applicable consumer protection or anti-money-laundering regulations.

An attempt to limit a regulated exchange's activities to one or another cryptocurrency would likely backfire. Users may prefer another and simply find access to exchanges based elsewhere that are willing to deal in the cryptocurrency of their choice. Additionally, the proliferation of several competing cryptocurrencies is indicative of a highly innovative market. Favoring one or another will discourage innovation, and leave that country's citizens less able to capitalize on the job growth and enhanced consumer services that experimentation with newer technologies and networks will bring.

6. Ensuring that regulatory requirements are reasonable

When applying any particular regulatory framework to users of these technologies it's important to be conscientious of what is and what is not possible or feasible to require from regulated firms. For example, if a company that deals primarily with cryptocurrencies is required to have a minimum net worth or minimum capital on-hand to guarantee its solvency, then it should be permitted to hold that capital in the form of cryptocurrency. If there is a statutory or regulatory definition of what kinds of investments are permissible for maintaining minimum capital, then that definition may need to be revised to include these new assets.

Similarly, in the anti-money-laundering context, it is critical to avoid mandating recordation or reporting of information that would not be reasonably available to the business. For example, a Bitcoin exchange will have information about its own customers (*e.g.* name, address,

transaction history, etc.), but it will generally not be able to determine any information about the persons from which its customers receive payment on the open Bitcoin network. If the payer is not a customer of the exchange, the exchange has no ability or legal reason to obtain information about them. The extension of existing anti-money-laundering norms to cryptocurrency exchanges should be considered accordingly.

We hope the foregoing is useful to you as you deliberate on the appropriate regulatory or self-regulatory approach to these new technologies. I also encourage you to review the many plain English explainers and policy white papers available on our website, coincenter.org. And if we can ever be of assistance, please do not hesitate to contact us.

Sincerely,

Jerry Brito
Executive Director