Regulating cryptocurrency exchanges

Cryptocurrencies are borderless and often transcend regulatory classifications. Establishing information sharing and coordination mechanisms between regulators and enforcement agencies is therefore crucial

Updated: June 1, 2020 9:27:23 pm

In its heyday, MT Gox crypto exchange accounted for nearly 70 per cent of all Bitcoin transactions. (Representational image)

Written by Radhika Pandey and D Priyadarshini

By striking down the Reserve Bank of India circular of April 6, 2018, the Supreme Court has given a fillip to crypto exchanges in the country. The circular had stopped traders and exchanges from accessing the banking system. Unable to conduct trades, several exchanges had shut down or moved overseas. Now, some have returned, others are seeing increased users and one has recently secured a multi-million dollar investment.

But the judgment has also rekindled the question of regulating crypto exchanges. There exists no clear legal and regulatory framework governing them. Recent reports suggest that the government may be mulling over a regulatory framework for cryptocurrencies. The RBI has also recently clarified that banks are not prohibited from providing services to traders and exchanges. Given the above, this article examines the broad contours of the possible approaches that can be taken to regulate crypto exchanges as they perform important functions but also carry significant risks.

Similar to stock exchanges, crypto exchanges provide an online platform or marketplace, albeit for cryptocurrencies. By also enabling trade or exchange of cryptocurrencies for fiat money, they connect the crypto and traditional financial systems. Regulators also look to exchanges for information on users and transactions, although this may depend on their organisational structure and functions. For example, centralised exchanges offer a single point of regulation. They have an entity in charge of the platform's governance and act as an intermediary throughout the trading process, namely, storing clients' funds, monitoring trades and ensuring fulfilment of orders. But decentralised exchanges enable trades or exchanges on a peer-to-peer basis through an automatic process involving smart contracts. They make regulation challenging due to the anonymity of users and lack of central presence.

Crypto exchanges have also assumed importance due to their role in initial exchange offerings (IEO). Unlike initial coin offerings where the issue of coins or tokens is made directly to investors, with the latter responsible to assess the project's credibility, crypto exchanges intermediate and vet

an IEO through due diligence of projects and KYC scrutiny of issuers. Crypto exchanges have therefore emerged as a key market infrastructure within the crypto-ecosystem.

But there are several concerns due to which regulation and supervision is required. In its heyday, MT Gox crypto exchange accounted for nearly 70 per cent of all Bitcoin transactions. Its hacking led to losses estimated in billions of dollars today. It went bankrupt. Investors' claims are yet to be settled. More recently, the sudden death of the CEO of Canada's largest exchange in India left millions of investors' money inaccessible in offline wallets. He alone knew the passwords. Such instances highlight some of the key risks associated with crypto exchanges — the safety and security of cryptocurrencies and lack of investor/consumer protection in the form of recourse, and quick and orderly access to their own funds/assets.

Moreover, unlike traditional securities markets, crypto exchanges perform additional functions like custody of assets or funds, clearing and settlement. They are also known to co-mingle client and proprietary funds or assets sometimes. Such practices, without adequate internal checks and controls, lead to conflicts of interest, micro-prudential and consumer protection risks.

Of particular concern is the un-intermediated access given to retail investors of complex products without adequate disclosures or advice regarding their suitability. The borderless nature of cryptocurrencies and service providers (like wallets and payment processing) weaken the ability to enforce investors' rights and recover their assets. Crypto exchanges are also known to enable circumvention of capital controls and commission of financial crime including money laundering and terrorism financing.

International experience illustrates some broad principles for regulating crypto exchanges. Typically, in jurisdictions that categorise cryptocurrencies as securities or other financial instruments, licensed crypto exchanges have emerged as a point of regulation, including for the implementation of anti-money laundering (AML) and terrorism financing (CFT) laws. Recognition then entails the application of existing securities laws as in the case of the US, UK, Japan or Hong Kong, or laws specifically designed for cryptocurrencies like Malta. International standard setting bodies like FATF and IOSCO too have provided guidance from time to time. Pertinently, IOSCO's recent report on cryptocurrency trading platforms recognises that risks currently associated with trading on such platforms and traditional risks in securities trading are similar. The report also notes that securities laws objectives like consumer protection and market integrity continue to apply even if underlying technology and business models of crypto exchanges pose unique challenges.

Accordingly, a legal and regulatory framework must first define cryptocurrencies as securities or other financial instruments under the relevant national laws and identify the regulatory authority in charge. Regulation must then define the entry points — who can carry out crypto exchange and intermediary functions, who can trade and what can be traded. Operation of crypto exchanges or intermediaries like brokers or custodians can be subject to receiving regulatory licenses. Licenses may be issued based on compliance with eligibility requirements and a detailed scrutiny of operational policies and procedures on internal governance, risk management and financial resources. Trading can be restricted to approved cryptocurrencies as in the case of Japan. Exchanges can be required to screen undesirable cryptocurrencies that don't permit tracing or are vulnerable to cyberattacks. Regulations can also require the performance of stringent KYC checks and independent verification by exchanges before onboarding investors. Access to retail or unsophisticated investors can be prohibited (like Hong Kong) or intermediated through professional advisors.

Thereafter, regulation must provide for ongoing supervision on matters concerning safety and security of assets and funds, transparency of operations including trading and price discovery, comprehensive and timely disclosures on the cryptocurrencies traded including risks and suitability for retail investors, and compliance with AML/CFT requirements. Record keeping, inspections, independent audits, investor grievance redressal and dispute resolution may also be considered to address concerns around transparency, information availability and consumer protection. Ongoing regulation and supervision seek to reduce the possibility of exchanges failing. But when they do, regulation must enable investor protection through quick and orderly access to their funds or assets.

Cryptocurrencies are borderless and often transcend regulatory classifications (as security, commodity or payment mechanism for example). Establishing robust information sharing and coordination mechanisms between regulators and enforcement agencies within the country, and with relevant foreign agencies would therefore be crucial too.

The writers are fellows at the National Institute of Public Finance and Policy