Challenges in regulating cryptocurrencies

Cryptocurrency transactions have led to concerns regarding consumer protection, money laundering, and financing of criminal activities

RADHIKA PANDEY AND BHAVYAA SHARMA
are consultants at the National Institute of Public Finance and Policy.

BLOOMBERG

A statement by the ministry of finance on cryptocurrencies warned investors to “stay away from such Ponzi schemes” as there is a “heightened risk of investment bubble of the type seen in Ponzi schemes”. This is the latest in a series of warnings and advisories issued by the government and the central bank in India. Countries across the world are grappling with the choice of an optimal regulatory framework in this field. Any regulatory framework in this field requires a comprehensive understanding of the functioning and structure of cryptocurrencies.

At the outset, it is essential to understand the difference between virtual currencies (VCs)—a term now synonymous with cryptocurrencies—and electronic money. While electronic money is legal tender that can be stored on a chip, VCs are a form of money or currency which does not derive its value from any sovereign authority, but by its technology. More specifically, cryptocurrency relies on principles of cryptography to implement a decentralized peer-to-peer ledger.

The key ideas that underpin bitcoin have been elaborated upon in its creator, Satoshi Nakamoto’s 2008 white paper, where bitcoin was introduced as an electronic, peer-to-peer, fully decentralized cash system, which does away with the need for a centralized entity. Since the validity of a transaction is arrived at through solving a computationally challenging exercise based on a cryptographic hash (known as proof of work), any malformed transaction is rejected by the participants (or miners) who keep working on finding the next valid block, after the successful completion of which they are rewarded with a transaction fee and a newly issued unit of currency. Transactions in this network are identified by public-private keypairs—a string of letters and numbers used to protect messages cryptographically.

These widespread cryptocurrency transactions have also led to concerns regarding consumer protection, money laundering, and financing of criminal activities. By design, cryptocurrencies allow anonymous funding; potentially acting as conduits for money laundering and terror financing. The consumer protection, in particular retail consumer protection concerns, stem from their volatile nature.

The clamour around regulation of cryptocurrencies poses a pertinent question: what is the optimal policy choice? Is a ban potentially more fruitful than regulation? Even if regulated, will the execution be foolproof? These are valid concerns, aggravated by the pace of evolution of this technology, which has outstripped regulation.

To be sure, there is no physical existence of money in the forms of notes, or cash, or gold bars. As a result, regulatory jurisdiction becomes complicated. One might argue that the location of the public-private keypair, the pseudonym identifying the transaction, could serve as a basis for regulation. However, not only is such a key non-existent physically, it could further be split into multiple components and spread across the globe, physically and electronically. Unless there is a robust de-anonymization framework, identifying the individual will not be easy, especially with the prevalence of remote servers. The most centralized channel to control the transactions and speculation would be to control the exchanges. Many exchanges in India and other countries follow “know your customer” and other regulatory mandates, which grants the investors significant protection while maintaining their privacy.

While the location of exchanges simplifies the question of jurisdiction, possibilities exist where an individual transfers coins from their private wallet in Country A, to buy goods in Country B through an exchange located in Country C. Even though the actual value is being transferred between Country A and Country B, the virtual currency transaction is taking place across Country A and Country C and from Country C to Country B.

The determination of location has important implications for cross-border payments’ purposes. Since virtual currencies enable quick transfers of huge amounts of money, regardless of the location of the payer and the payee, the threshold of permissible cross-border transaction amounts could be different. Taxation-related issues also become more complex. The Internal Revenue Service in the US treats cryptocurrencies as “property”, hence making them applicable to capital-gains tax, while bitcoin mining is subject to self-employment tax regulations. The recent legislation in South Korea subjects income from cryptocurrency trading to capital taxation rules. Again, if the public-private keypair is stored at one location, then the tax jurisdiction is clear. If however, the key is split into multiple parts and stored at different locations, the applicable tax would need to be reconciled with the taxation laws of all these locations.

While the ability to mask identities while performing transactions in cryptocurrencies has led to suspicion, the reassuring part emerges from the underlying technology of cryptocurrencies itself—blockchain. The fundamental difference between pseudonymity and anonymity is worth reiterating. The public-private keypair assures that the transaction leaves traces on every node (or system) which stores the blockchain, and can be linked to real-world identities using transaction-graph analysis.

There is a clear message for governments and regulators —step up your technology or you will lose. Banning cryptocurrency mining or trading would eliminate financial incentives to further the distributed ledger technology and restrict the positive spillovers in the field of healthcare, finance, governance and so on.

However, an active effort in linking research to policymaking to better understand the implications of cryptocurrencies and its underlying technologies would be optimal.

Comments are welcome at theirview@livemint.com