# Technology issues behind cryptocurrencies

*The issue of a parallel economy on cryptocurrency networks has caused governments to take a stern view on cryptocurrencies*

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

In a recent move, the Reserve Bank of India (RBI) barred banks and other regulatory entities from dealing with cryptocurrency dealers. In January, a cyber law expert filed a public interest litigation with the Calcutta high court, demanding a proper framework to regulate cryptocurrencies. These developments have brought the potential risks associated with cryptocurrencies to the fore. While researchers and stakeholders are exploring the benefits of cryptocurrencies and their underlying technologies, the volatility and the susceptibility to attacks cloud the many potential benefits that they can offer. The risks associated with cryptocurrencies are becoming increasingly evident, along with their potential benefits, thus underscoring the need for a proper understanding of technical issues, which are imperative for robust solutions.

A few comprehensive user surveys over the bitcoin network highlight the various uses it is put to by individual participants and companies. In one such survey, a majority of the participants reported using bitcoins for tips and donations, followed by purchase of virtual goods and services. A very small proportion admitted to purchasing drugs. On the question of risk perceptions, users around the world mainly consider value fluctuation, followed by glitches in wallets and malware attacks as the primary risk factors. Several instances of security breaches and loss of cryptocurrencies over the network have surfaced in the recent period.

While loss over the private keys could be because of lack of understanding by individuals and inability to password-protect their wallets, exchanges, which are a point of centralization in an otherwise decentralized network, have become more susceptible to double-spending attacks. The most famous example of this is the Mt Gox hack. In 2014, the then largest bitcoin trading exchange suddenly faced a technical collapse, after which thousands of consumers found out that approximately $460 million worth of cryptocurrencies had been wiped out by hackers. Only a small proportion has been recouped, but the incident was a glaring example of how strong the vulnerabilities in the system are, and how devious mechanisms can exploit them to erode a huge chunk of global savings.

If the private keys of the hackers can be traced, the authorities can recover the money. But if the tracing and linkability is not possible, then surely the money is lost. There is no mechanism of insurance to absorb such losses, and with the evolution of such attacks, it has become imperative for exchanges, like other financial institutions, to create more robust systems to avert such incidents of cyber attacks.

Another cause for vexation amongst onlookers of the cryptocurrency evolution is the associated pseudo-anonymity and the channels it offers to criminal activities, including money laundering and drug trafficking. The biggest example is the Silk Road scandal. In the US, Silk Road was an online black market that facilitated transactions in illegal drugs by anonymous users. However, this very pseudonymity also invited attention from different fields, including healthcare and governance, where the privacy of consumers and citizens of the country is protected within a permissioned blockchain.

The issue of a parallel economy on the cryptocurrency networks has also caused governments to hold a stern attitude towards cryptocurrencies. However, since the underlying blockchain broadcasts a new transaction whenever it is verified under the consensus systems, some level of traceability may be possible. For instance, transactions broadcasted on the bitcoin network hold information on pseudonyms or the public-private keys of transactors, which are addresses to which the coins are transferred. Linking address clusters of the sellers or buyers on the cryptocurrency network to real-world identities is possible.

Another linkage is possible through the IP addresses of the participants. This is where the IP-address-shielding technologies like Tor (essential to the dark web) come in, which, due to their ability to shield the network addresses of the participating systems on the network, could pose difficulties in detecting criminal activities. However, research efforts have been successful in disconnecting the linkage between Tor and cryptocurrency networks, as well as de-anonymizing the perfectly encrypted cryptocurrencies.

Regular protocol updates, of the software that governs rules, operations, and communication between network nodes, are essential to the functioning of blockchain-based technologies. Any change in the existing blockchain, even if it is through a consensus and not an attack, can raise fungibility and security issues. At the same time, such updates might be necessary to ensure the efficiency of the existing peer-to-peer decentralized systems.

Users and traders need to be aware of such updates to be informed of their future repercussions. Such protocol updates should aim at impeding the movement of malicious parties, which can damage the integrity of the blockchain if they hold more than 50% of the computing power on the network. The onus is on the core developers to have in place a process that leverages the existing consensus systems to resist such attacks.

The technical challenges associated with cryptocurrencies are numerous, but a thorough understanding by all the stakeholders will ensure that such issues are not only resolved through successive updates but robust systems are put in place, which can allow socially optimal positive externalities to be generated.

*Comments are welcome at theirview@livemint.com*

AFP