Cryptocurrencies and the Regulators Dilemma

More from the author

When Satoshi Nakamoto (a pseudonymous person or group) published the pioneering paper *Bitcoin: A Peer-to-Peer Electronic Cash System* in 2008, he/they would have hardly anticipated that the valuation of the cryptocurrency – Bitcoin – founded a year later would surge to 2300 USD[1] a unit in less than a decade. At present, there are around 969 cryptocurrencies in existence across the globe, with a total market capitalisation close to 116 Billion USD.[2] Founded as a peer-to-peer electronic payment system, cryptocurrencies enable transfer of money between parties, without going through a banking system. These digital payment systems are based on cryptographic proof of the chain of transactions, deriving their name, Cryptocurrency. These employ cryptographic algorithms and functions to ensure anonymity (privacy) of the users (who are identified by an alphanumeric public key), security of the transactions and integrity of the payment systems. "Decentralised Digital Currency" or "Virtual Currency" is also interchangeably used for a cryptocurrency.

Widely seen as a disruption for the traditional banking and financial institutions, cryptocurrencies have gained significant traction over the last half a decade, at the same time creating a regulatory nightmare for banking regulators across the globe. Governments and their regulatory bodies have been brainstorming for measures to either regulate the growth of cryptocurrencies, as against just letting them proliferate without regulation and interference. While the US Senate had a hearing on Bitcoins in 2013, the Canadian Senate's Standing Committee on Banking, Trade and Commerce carried out an extensive study on the use of digital currency in 2014. The acceptability of cryptocurrencies as a legal instrument currently varies from country to country; while some are in the process of formulating laws and measures, others are yet to respond to this disruptive change. The burgeoning use of cryptocurrencies in terror financing, ransomwares, illicit drugs or arms trade and cybercrime has also raised red flags among the security and law enforcement agencies.

The Reserve Bank of India has been keeping a tab on the increasing use of cryptocurrencies and it had issued an advisory in this regard in 2013, cautioning users, holders and traders of virtual currencies to its potential financial, legal and security related risks.[3] The Ministry of Finance also held a public consultation on regulating virtual currencies in May 2017. The overarching issues of regulation, monitoring, measures for consumer protection and security pose a dilemma before the regulatory bodies.

Cryptocurrency is fundamentally a decentralised digital currency transferred directly between peers and the transactions are confirmed in a public ledger, accessible to all the users. The process of maintaining this ledger and validating the transactions, better known as *mining,* is carried out in a decentralised manner. The underlying principle of the authenticity of the present to historical transactions is cryptographic proof, instead of trust; different from how it happens in the case of traditional banking systems.

Any exchange of currency, between party A and party B is a transaction. A cryptographic algorithm/function encrypts this transaction using the digital signatures of the parties to establish their authenticity. Once validated, the transaction reflects in the public ledger, maintained by so-called miners. Cryptocurrencies also bring in transparency in transactions, and all transactions, from the day the first unit of currency was rolled out, are stored in this public ledger. As a privacy measure, the transactions do not reveal the identities of the parties, but rather uses their cryptographic signatures or hash to identify them while mainatianing their anonymity. The transactions do not disclose any details of the parties, be it the name, gender, location signature, credentials or nationality.

The architecture of cryptocurrencies engrain the concepts of cryptography and protocols which are based upon the principles of advanced mathematics and computer engineering. This makes cryptocurrencies secure and hard to duplicate or counterfeit.

Another aspect that enshrines transparency in the cryptocurrencies is the extensive use of open source software. Mining, the process of ledger keeping and validating transactions, is also a truly decentralised and distributed process, open to everyone. The architecture of the software and system behind cryptocurrencies ensures the integrity of transactions, blocks of the transactions, and the public ledger.

The prominent feature in the design of cryptocurrencies architecture is decentralised control, which means, no single authority, institution, individual or group controls the flow of transactions, supply or valuation of the currency. Rather, the collective computing power of the miners ensures seamless operations while demand-supply dynamics drive the valuation, which is further governed by the protocols built into the software of the cryptocurrency.

The following concepts govern the functioning of most of the cryptocurrencies, however, they all vary in some way or the other in terms of development and implementation of the software or business rules:

Proof-of-work in the case of Bitcoin is finding a number, *nonce*, when added to the block, the block hash begins with a specific number of zero bits. This is more of a random search, and the probability of successful generation is really low, making it unpredictable which node in the network will be able to generate the next block. The required computation increases exponentially as the number of initial zero bits required increases.5 At present, SHA-256 is the most widely used hash algorithm for proof-of-work, while others are Scrypt, Blake-256, HEFTY1, Quark, SHA-3 and so on.

A blockchain is a sequence of interconnected blocks of finite transactions over a period of time, which could vary from a minute to a few hours or even a few days, depending upon the volume of the transactions. All the transactions within the finite time frame form a block, whose signature or hash (SHA-256 in the case of Bitcoin) is computed and interlaced with the next block, therefore forming a chain of blocks, which ensures the integrity of a cryptocurrency. In essence, a blockchain is a pubic ledger, which is distributed, synchronised and secured by cryptography. This digital ledger in maintained in every node of the network by the miners supporting the operations of cryptocurrency.

Blockchain is fundamentally a technology which not just empowers cryptocurrencies, but has found diverse applications as a digital ledger providing a secure way of making and recording transactions, agreements, contracts and land records. Being a digital ledger, a blockchain can be decentralised and distributed, enabling storage of multiple copies across the network.

Like cryptocurrencies, , the underlying blockchain technology is also considered to be a disruptive innovation. Blockchain is transparentand can maintain an indisputable record of transactions, and could potentially be used for a variety of purposes, including maintaining land tenure records and property rights.7 Exploratory research is going into creating blockchain applications in banking, pharmaceuticals, stock markets and software for supply chain integrity, maintaining contacts, banking transactions and to curb digital piracy.

Cryptocurrencies blend the best of all the above technologies or processes to offer the users an open-source, cryptographically secure platform for transactions and/or making payments which preserves their privacy and has diverse utilities. The transactions on these platforms might be a small fraction as compared to traditional banking systems, but with the growing penetration of

smart phones and internet connectivity, this innovation might seriously challenge this segment of financial sector once it moves up the value chain.

Professor Clayton Christensen had coined and defined the term *Disruptive Innovation* as a "process by which a product or service takes root initially in simple applications at the bottom of a market and then relentlessly moves up market, eventually displacing established competitors." There have been numerous instances where disruptive technologies have displaced well-established competitors, WhatsApp displacing Short Messaging Service (SMS) being one such example. Disruptive technologies offer value to the users, in terms of cost-effectiveness, usability and simplicity.8 Considering cryptocurrencies in this perspective , they may well have the potential to displace the existing financial systems which enable electronic flow of money across different political boundaries. The success of cryptocurrencies could be attributed to the advantages they have, such as:

Another facet, which brings the cost down considerably low, is inbuilt security and fraud prevention mechanism, which accounts for 40% of the costs of payment processing gateways.11

Despite these numerous advantages and user friendly processes, cryptocurrencies have their own set of associated risks in the form of volatility in valuation, lack of liquidity, security and many more. Cryptocurrencies are being denounced in many countries because of their use in grey and black markets. There are two sets of interconnected risks; one being to the growth and expansion of these platforms in the uncertain policy environment, and the other being the risks these platforms pose to the users and the security of the state.

In 2014, hackers stole about 480 million USD in Bitcoins from Tokyo's Mt. Gox exchange;14 which, at that time, was one of the biggest Bitcoin exchange in the world. There have been many more such incidents in recent times; attackers moved about 60 million USD worth of the virtual currency Ether from the account of Decentralized Autonomous Organization (DAO) in June 2016;15 a breach at Bithumb, South Korea's largest Bitcoin and Ethereum exchange, led to a loss of around 1 million USD worth of cryptocurrencies in June 201716; and hackers hijacked cryptocurrency trading platform CoinDash in the middle of its initial coin offering and stole 7 million USD from CoinDashon 17 July, 2017.17 In general, the reported instances of thefts have been from the exchanges or the users' end. Users are prone to the risk of losing their holdings if they lose the private encryption key or forget it or lose the storage device/hardware where the wallet is kept or even lose the key due to a theft or hack.18

Additionally, cryptocurrency platforms have also been found to be prone to DDoS attacks, targeted at the exchanges might slow down services or render the platform completely inaccessible. Bitfinex, a Bitcoin exchange, faced DDoS attacks in February 2017; Indian exchange Coinsecure had faced similar attacks in 2016, and BTC-E, Krazen, Poloneix have been a victim of DDoS attacks.20 Owing to these threats, cryptocurrency founders/firms have rolled out a Cryptocurrency Security Standard, a set of requirements for all information systems that make use of cryptocurrencies, including exchanges, web applications, and cryptocurrency storage solutions, complementing existing information security standards such as ISO 27001:2013.21

Perhaps, unless and until these risks are mitigated, the future of cryptocurrencies as legal instruments for exchange or goods and services or for that matter, payments, will continue to remain uncertain. Some of these are technical challenges, such as dispute settlement and security of platforms, while others are policy issues which are much more difficult to resolve such as regulation, liquidity, price volatility and consumer protection. Moroever, cryptocurrencies are an entirely new payment method, with privacy benefits for users, but at the same time, this poses significant risks to security practices , counter-terrorism, law enforcement and taxation.

The policy response to changes in financial sector is state driven, and the governments take cautious steps especially when it is a case of disruptive technology, having the potential to disrupt existing institutions, policies, strategies and practices. Regulatory agencies are still weighing the issue through the lens of consumer protection and money laundering/terror financing. The government of India and its regulatory body, the Reserve bank of India have been following the developments in this sphere for quite some time. The RBI, in 2013, had issued a warning to individuals dealing with virtual currencies in India on the financial, legal, operational and security-related risks, and warned that this could even subject the users to unintentional breaches of anti-money laundering and combating the financing of terrorism (AML/CFT) laws.37 It further reiterated this stand in 2017, again cautioning users, holders and traders of Virtual Currencies about the potential financial, operational, legal, customer protection and security related risks.38 The RBI clarified that it has not given any licence or authorisation to any entity/company to operate such schemes or deal with Bitcoin or any virtual currency.39 Owing to the rising concerns, the government of India has set up a committee to take stock of the present status of Virtual Currencies both in India and globally; examine the existing global regulatory and legal structures; and suggest measures (related to consumer protection, money laundering, etc). The committee, chaired by the Special Secretary (Economic Affairs) has representation from Department of Economic Affairs, Department of Financial Services, Department of Revenue (CBDT), Ministry of Home Affairs, Ministry of Electronics and Information Technology, Reserve Bank of India, NITI Aayog and State Bank of India.40 The committee is expected to roll out its report by the end of July.

In May 2017, based on the deliberations of this committee, the Department of Economic Affairs had invited comments from members of public for wider consultation and solicited inputs through MyGov platform41, which received 4,000 comments.42 Apart from this committee, there is also a Parliamentary Standing Committee on Finance which is looking into these developments. Questions regarding the developments in this sphere have regularly been tabled before the Ministry of Finance in both the houses of Parliament.43 As the legality and legitimacy of cryptocurrencies hangs in the balance, online cryptocurrency exchanges have mushroomed in India, facilitating their sale and purchase. These are self-regulated trading platforms, employing strict customer identification procedures such as Know Your Customer (KYC), and monitoring transactions of suspicious nature to dissuade money laundering, terror financing or other criminal activities.44 Going a step forward, these start-ups have even formed their association – the Digital Assets and Blockchain Foundation India, working towards awareness and best industry practices.

There are three probable directions in which the future discourse on cryptocurrencies will advance; that governments will: a) let cryptocurrencies proliferate as per the market dynamics, without any intervention; b) regulate this segment, designate a status such as legal instrument or capital asset with safeguards for protection against the risks like terror financing, illicit trade or tax evasion; c) proscribe them, given the security risks to the state and perils to the users from volatility, liquidity and security of the assets/systems.

Given the arising interest and enthusiasm of wider populace, technology entrepreneurs and legislators, proscribing cryptocurrencies is unlikely to happen in India. Also, the inherent risks to the security and economy of the state, as well as to the users will dissuade the government from letting cryptocurrencies proliferate without regulation. Therefore, it is quite likely that the further growth and development of cryptocurrencies in India, and their integration with the financial system, if at all, will be regulated under close observation and scrutiny, particularly in the initial phase. Nevertheless, the three factors which are going to shape the likely outcomes of policy on cryptocurrencies in India are:

For developing countries like India, disruptive technologies like cryptocurrencies bring their own set of benefits and risks. At one end, traditional banking systems have their constraints regarding

reach and innovation, where private enterprises fill this space up with novel ideas and innovative business solutions. At the other end, developing countries are at the lower end of technology adoption life cycle, as far as design, development or entrepreneurship in disruptive technologies is concerned. These countries are generally caught by surprise, as disruptive innovations suddenly rise up the value chain and rattle their existing policies, processes, strategies, instruments or technologies. Cryptocurrencies could be a great value proposition in this regard for India, but the prominent security threats, in form of terrorism and left wing extremism, might bring in some hesitation in the early phase of adoption or integration of this technology with the financial system.

If authorised as an electronic payment system or designated a legal instrument, cryptocurrencies will fall under the purview of the RBI; capital gains and business transactions will be liable to tax, and foreign payments are also going to fall under the auspices of Foreign Exchange Management Act. Regulated cryptocurrencies will enshrine robust consumer protection provisions. In terms of benefits, this could be a force multiplier in India's quest for financial inclusion, parallel to the electronic payment modalities such a digital wallets and Adhaar Enabled Payment System. It could further reduce the cost associated with remittances, which brings annual earnings of close to 62 billion USD to India,45. It would also attract future business entrepreneurs, leading to innovation, generation of job and wealth creation in the due process of payments processing, e-commerce and taxation.

Cryptocurrencies are a disruptive innovation that have already begun to alter the existing means of electronic payments, money transfers, policies and regulations. India has also moved a step forward in this regard by considering legalising of these currencies. If the further growth of cryptocurrencies is regulated in India, there will be certain requisites such as a registration process (KYC norms), scrutiny of transactions (in the form of mandatory bank transfers for sale of cryptocurrencies or quoting of Permanent Account Number/Adhaar); reporting/declaration of profits/sales/gains from trading or business activity in cryptocurrencies. The government will have to take considered steps, given the risks from possible use of cryptocurrencies in terror financing, money laundering and tax evasion. Such regulation would still not address the looming risks from price volatility, security breaches and the lack of consumer protection mechanisms, due to prevalent constraints pertaining to the jurisdiction and authority over cryptocurrencies.

Views expressed are of the author and do not necessarily reflect the views of the IDSA or of the Government of India.

available at https://www.cryptocoinsnews.com/antonopoulos-answers-inevitable-bitcoin-terrorism-question/, accessed on July 18, 2017.

b) Question (no. 1142) by Smt. Meenakashi Lekhi in Loksabha on Bitcoin Currency, April 29, 2016, available at http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=33353&lsno=16, accessed on July 20, 2017.

c) Question (no. 523) by Shri. Parvesh Sahib Singh in Loksabha on Regulation of Bitcoin, November 18, 2016, available at http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=41144&lsno=16, accessed on July 20, 2017.

d) Question (no. 335) by Shri. Jose K. Mani in Loksabha on Bitcoin Currency, February 03, 2017, available at http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=46362&lsno=16, accessed on July 20, 2017.

END