INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

IDSA
Special Feature

Cryptocurrencies and the Regulators Dilemma

Munish Sharma

August 1, 2017

Summary

Cryptocurrencies have already begun to disrupt the traditional ways of banking, money transfers, monetary policies and regulations across the globe. As cryptocurrencies gain significant traction, governments and their regulatory bodies have been brainstorming for measures to regulate this burgeoning sphere of virtual currencies. Like all disruptive innovations, cryptocurrencies bring both risks and opportunities in their wake. This special feature explores the mechanics and attributes which have led to the steep rise of cryptocurrencies, delves into the risks they pose to the user and the state, and evaluates the opportunities, risks and policy options for India.

Introduction

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.

---

1 Bitcoin Price, available at http://www.coindesk.com/price/, accessed on July 10, 2017.

2 Cryptocurrency Market Capitalisation (as of July 2017), available at https://coinmarketcap.com/all/views/all/, accessed on July 10, 2017.

3 Reserve Bank of India, "RBI cautions users of Virtual Currencies against risks", December 24, 2013, available at https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247, accessed on July 05, 2017.

The Mechanics of Cryptocurrencies

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:

- **Decentralised**: Majority of the fiat currencies in circulation are controlled by a government or a regulatory body, and their creation can be regulated, based on the internal calculations, forecasts or requirements of the regulatory or government

backing the currency. This is different in the case of cryptocurrencies, whose creation and transactions are open source and publicly available, controlled by the software code which is again open source, and rely on "peer-to-peer" networks, rather than a centralised agency or authority. There is no single entity that can affect or manipulate or regulate any of these aspects of the cryptocurrency.

- **Digital**: Cryptocurrencies are completely digital – they could be stored in digital wallets and transferred digitally to other peoples' digital wallets or stored on a computer device, a pen drive or a hard drive. The transactions are also digital – with a public record of the transactions on the network.
- **Open Source**: Cryptocurrencies developed with the open source methodology have their software source code available for open review, integration, development and enhancement. Developers can create Application Programming Interfaces (APIs) with cryptocurrencies without paying a fee and they are open for everyone to use or join the network, irrespective of nationality, gender or location.
- **Miners** are the backbone of a cryptocurrency. Miners pool in hardware and computing power and collectively verify the authenticity, accuracy, and security of the blockchains. As the blockchain grows, so does the complexity demanding tremendous amounts of computing power and electricity to power these computers. Every new block in the chain brings a monetary reward to the miner whose block is accepted, and this injects wealth into the cryptocurrency system. The process of mining also generates value for the miners in the form of transaction fees, which is optional and very low as compared to traditional banking systems.
- **Proof-of-work** is just a small set of data which is difficult to compute but quite easy for others (peers) in the network to verify. Miners have to complete a proof-of-work on the present block of transactions, for their block to be accepted by other nodes in the network as legitimate. The difficulty of this proof-of-work adjusts based on the business rules of the software, which sets the approximate time limit to a new block. Proof-of-work difficulty is determined by a self-adjusting target, based on the average number of blocks per hour. If the blocks are being generated too fast, difficulty increases.[4]

  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

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *Bitcoin*, available at https://bitcoin.org/bitcoin.pdf, p. 3, accessed on July 10, 2017.

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 **cryptographic hash** is like a fixed size signature for a set of text or a data file. SHA-256 algorithm, as like many other cryptographic hash functions, generates an almost-unique, 256-bit (32-byte) hash of the input file or text. Hash is a basically one way function – it cannot be decrypted back. This makes hash algorithms suitable for password validation, challenge hash authentication, anti-tamper and digital signatures.[6] Cryptocurrencies use cryptography to build trust and security safeguards.

- **Adaptive Scaling** built into Cryptocurrencies ensuring they can adjust to all kinds of loads. The algorithm adjusts the difficulty of the proof-of-work as per the dynamics of demand. As part of the algorithm, some of cryptocurrencies are designed to have a finite number of units to be mined over the course of time. For example, the circulation of Bitcoin is capped at 21 million units.

- **Blockchain Technology**: A blockchain is the electronic ledger which maintains record of all the transactions from the time the first unit of the cryptocurrency – the seed - was mined. Blockchain can validate the integrity of all the units of currency at any given point of time. As a protocol, each new block contains the hash of the preceding blocks, and this phenomenon links the previous blocks to the new block, thus forming a chain of blocks. This process validates each block, all the way to the genesis block, integral to the security and integrity of the database.

  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.

---

5 Ibid.

6 SHA-256 Hash Calculator, available at http://www.xorbin.com/tools/sha256-hash-calculator, accessed on July 10, 2017.

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.

Cryptocurrencies as a Disruptive Innovation

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:

1) **Privacy Protection**: Privacy and anonymity of the transacting parties was the prime concern of the proponents of cryptocurrencies when the idea was promulgated, and these became part of the underlying principles. The use of pseudonyms conceals the identities, information and details of the parties to the transaction – perquisites for privacy enthusiasts.

---

7 Katherine Purvis, "Blockchain: What is it and what does it mean for development?", *The Guardian*, January 17, 2017, available at https://www.theguardian.com/global-development-professionals-network/2017/jan/17/blockchain-digital-technology-development-money, accessed on July 10, 2017.

8 Timothy B. Lee, "Bitcoin is a Disruptive Technology", *Forbes*, April 9, 2013, available at https://www.forbes.com/sites/timothylee/2013/04/09/bitcoin-is-a-disruptive-technology/#995cc6e29562, accessed on July 10, 2017.

2) **Cost-effectiveness**: Electronic transactions attract fees and charges, which is on the higher side when the transactions are transnational and undergo currency conversion, or attract processing fee levied by the banks, third party clearing houses or gateways. Debit or credit card transactions also attract a processing or transaction fee when used overseas, which is somewhere of the order of 1% to 3%,[9] while electronic transfers could exceed to 10% or 15%[10]. Cryptocurrencies solve this problem, as they have single valuation globally, and the transaction fee is extremely low, being as low as 1% of the transaction amount. Cryptocurrencies eliminate third party clearing houses or gateways, cutting down the costs and time delay. All the transactions over cryptocurrency platforms, whether domestic or international, are equal.

   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]

3) **Lower Entry Barriers**: Possessing a bank account or a debit/credit card for international usage requires documented proofs for income, address or identification. Banks or financial institutions might have their own set of eligibility criteria for these facilities. Cryptocurrencies lower these entry barriers, they are free to join, high on usability and the users do not require any disclosure or proof for income, address or identity.

4) **Alternative to Banking Systems and Fiat Currencies**: Governments have a tight control and regulation over banking systems, international money transfers and their national currencies or monetary policies. Cryptocurrencies offer the user a reliable and secure means of exchange of money outside the direct control of national or private banking systems.

5) **Open Source Methodology and Public Participation**: A majority of the cryptocurrencies are based on open source methodology, their software source code is publicly available for review, further development, enhancement and scrutiny. The ecosystem of cryptocurrencies is primarily participation based, as software development, bug reporting and fixing, testing etc. are driven by the wider user base, rather than a closed set of individuals or an institution. They have their own consensus

---

9 Foreign Transaction Fee: What is it? and how does it work?, available at https://www.valuepenguin.com/credit-card-foreign-transaction-fees, accessed on July 10, 2017.

10 Katie Lobosco, "Walmart offers less costly money wire service", *CNN Money*, April 17, 2014, available at http://money.cnn.com/2014/04/17/news/companies/walmart-money-transfers/, accessed on July 10, 2017.

11 Andreas M. Antonopoulos, Consensus Algorithms, Blockchain Technology and Bitcoin UCL, *Youtube*, January 31, 2016, available at https://www.youtube.com/watch?v=fw3WkySh_Ho, accessed on June 15, 2017.

based decision making, built-in quality control and self-policing mechanisms for building frameworks, practices, protocols and processes.

6) **Immunity to Government led Financial Retribution**: Governments have the authority and means to freeze or seize a bank account, but it is infeasible to do so in the case of cryptocurrencies.[12] For citizens in repressive countries, where governments can easily freeze or seize the bank accounts, cryptocurrencies are immune to any such seizure by the state.

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.

Risks involved in Cryptocurrencies

1. **Key/Wallet/Exchange Security**: A virtual wallet stores the keys and transaction records of the user. The secure digital keys are used to access the public address and to sign or authenticate the transactions initiated by the user. Virtual wallets exist in the forms of desktop wallets (a software), Web-based wallets (a website/cloud) and mobile wallets (an app). Cold storage of cryptocurrencies is claimed to be more secure, which is in the form of storage media, USB drive, on the paper or hardware wallets[13], with some of them even using biometrics for authentication. Specialised online exchanges facilitate the purchase or sale of cryptocurrencies. In the entire chain of security, wallets and exchanges are found to be the weakest link, and that is where the attacks are commonly aimed at.

   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

[12] Brian Martucci, "What is Cryptocurrency – How it works, History and Bitcoin alternatives", available at http://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/, accessed on July 14, 2017.

[13] Alexandr Nellson, "How to properly store Bitcoins and other cryptocurrencies", available at https://medium.com/@nellsonx/how-to-properly-store-bitcoins-and-other-cryptocurrencies-14e0db1910d, accessed on July 14, 2017.

[14] "Ten arrested in Netherlands over bitcoin money-laundering allegations", *The Guardian*, January 20, 2016, available at https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy, accessed on July 14, 2017.

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 2017[16]; 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]

2. **Hijacking/Routing Attacks/Distributed Denial of Service (DDoS) attacks on Cryptocurrency System**: Cryptocurrency systems are open source and the pooled in resources of the miners keeps these systems up and running. Some of the research efforts in the recent past have delivered proofs-of-concept for hijacking or Internet routing attacks to which cryptocurrency systems[19] are vulnerable to.

   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

---

15 Charles Cooper, "The cybersecurity of cryptocurrency", *CSO Online*, February 23, 2017, available at http://www.csoonline.com/article/3166938/data-breach/the-cybersecurity-side-of-cryptocurrency.html, accessed on July 14, 2017.

16 Japonica Jackson, "Largest cryptocurrency exchange hacked, over $1 million worth of bitcoin stolen", *IT Security Guru*, July 6, 2017, available at http://www.itsecurityguru.org/2017/07/06/largest-cryptocurrency-exchange-hacked-1-million-worth-bitcoin-stolen/, accessed on July 20, 2017.

17 Jen Wieczner, "Hackers Just Stole $7 Million in a Brazen Ethereum Cryptocurrency Heist", *Fortune*, July 18, 2017, available at http://fortune.com/2017/07/18/ethereum-coindash-ico-hack/, accessed on July 20, 2017.

18 Gautam Vora, "Cryptocurrencies: Are Disruptive Financial Innovations Here?", *Modern Economy*, 6, pp. 816-832, available at https://file.scirp.org/pdf/ME_2015072011152606.pdf, p. 818, accessed on July 20, 2017.

19 Maria Apostolaki, Aviv Zohar and Laurent Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies", available at https://btc-hijack.ethz.ch/, accessed on July 20, 2017.

20 JP Buntix, "Top 5 Cryptocurrency Exchanges hit by DDoS Attacks", *The Merkel*, May 30, 2017, available at https://themerkle.com/top-5-cryptocurrency-exchanges-hit-by-ddos-attacks/, accessed on July 20, 2017.

cryptocurrency storage solutions, complementing existing information security standards such as ISO 27001:2013.[21]

3. **Uncertain Regulatory Environment**: The future and further success of cryptocurrencies depends upon the way regulatory frameworks are devised. Different countries have approached this innovation in different ways, and therefore the regulatory environment remains uncertain.

4. **Lack of Liquidity and Lower Acceptability**: Cryptocurrencies function outside banking systems, beyond the regulations or controls of the regulatory agencies. Although online exchanges facilitate exchange of cryptocurrencies with fiat currencies, but generally, this is restricted to the more popular cryptocurrencies only, basically, the ones with high market capitalisation. For the rest of cryptocurrencies, and for all of them in certain countries, there is an absolute lack of liquidity. Moreover, the acceptance of cryptocurrencies at merchant sites is also restricted. As cryptocurrencies are gaining popularity and entering into niche markets, exchanges have sprung up dealing in national currencies such as Rupee, Yuan and Yen, adding much required liquidity to the cryptocurrencies, but still restricted to the popular ones.

5. **Price Volatility**: Volatility, a measure of variance of the price of a financial instrument over a certain period of time, is associated with the risk level of the instrument. High volatility is regarded as risky, and cryptocurrencies are known to be extremely prone to price fluctuations. The prices of Bitcoin touched an all-time high of 2,700 USD in May 2017, followed by a sharp correction, shedding around 30% of its value in the next two days.[22] There have been four of such rallies for Bitcoin, while others such as Ethereum, Litecoin, Dash, Ripple and Monero etc. have had their own price fluctuations. These fluctuations are driven by many factors, varying from geopolitical events to the policies or regulations of governments[23], from security breaches at exchanges to the vulnerabilities found in the code, or their reported use/abuse in illicit trade. Cryptocurrencies do not yet have an accepted vulnerability index, which other financial instruments such as fiat currencies and gold have. Experts believe and argue that, when the consumer base of these instruments widens, the market and prices of cryptocurrencies will automatically stabilise.[24]

---

21 CryptoCurrency Security Standard, available at https://cryptoconsortium.github.io/CCSS/, accessed on July 20, 2017.

22 Wassim Bendella, "Insufficient Understanding of Cryptocurrencies Results in Their Volatility", The Cointelegraph, June 11, 2017, available at https://cointelegraph.com/news/insufficient-understanding-of-cryptocurrencies-results-in-their-volatility, accessed on July 20, 2017.

23 Jonathan Todd Barker, "Why Is Bitcoin's Value So Volatile?", May 16, 2017, available at http://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp#ixzz4nLbQKy1h, accessed on July 20, 2017.

24 n. 22.

6. **Uncertainly over Consumer Protection and Dispute Settlement Mechanisms**: Cryptocurrencies are decentralised, that means, there is no single authority for mediation or dispute redressal. The miners are not responsible for any arbitration of disputes between the parties. The transactions are also irreversible, which, in the case of banks or payment gateways is reversible if the dispute is resolved, safeguarding the users from fraud. Cryptocurrencies lack these safeguards, exposing the users to the risks of fraud and bringing a sense of uncertainly over consumer protection and dispute settlement mechanisms.

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.

Risks from Cryptocurrencies

1. **Potential use for Illicit Trade and Criminal Activities**: The perpetrators of Wannacry ramsomeware - which created havoc across 150 countries in May 2017 - demanded ransom of 300-600 USD through Bitcoins. Cryptocurrencies are virtual and decentralised, well beyond the control or authority of the state. Probably, this has made their absorption quicker into grey and black markets, ransomwares and a host of other illicit activities of crime and money laundering. The infamous marketplace "Silk Road" over DarkWeb relied heavily on Bitcoins for payments in exchange of illicit trade of narcotics, hacking tools, small arms, child pornography, stolen credit cards information and so forth. Between 2011 and 2013, the value of Bitcoins surged as criminals were purchasing Bitcoins in large volumes.[25] In late 2015 and early 2016, Dutch police unearthed two small groups that indulged in Bitcoin-related money laundering.[26] Regulatory bodies and law enforcement agencies have raised legitimate concerns that cryptocurrency accounts and wallets cannot be frozen, seized or examined.[27] .

2. **Potential use for Terror Financing**: In the aftermath of the attack on World Trade Centre on September 11, 2001, rigorous vigilance and regulatory controls were

25 Paul Gil, "What Are Bitcoins? How Do Bitcoins Work?", *Lifewire*, May 26, 2017, available at https://www.lifewire.com/what-are-bitcoins-2483146, accessed on July 18, 2017.

26 n. 15.

27 n. 25.

imposed on global financial systems to crack down on terror financing. This moved terror outfits towards money laundering and hawala networks, but owing to the similar reasons as stated above, cryptocurrencies are also emerging as a new funding stream for terrorist outfits.[28]

In a blogpost, titled "Bitcoin and the Charity of Violent Physical Struggle[29]", Islamic State of Iraq and Syria (ISIS) had proposed using Bitcoins to raise funds., Known instances of terror outfits using these modalities are very limited, with one such instance emerging out of Indonesia recently.[30]

The proponents and entrepreneurs of cryptocurrencies, however, denounce the proposals of ban and control on cryptocurrencies, as they argue that many technologies such as smartphones are also being used by terrorists and criminals, and they are not liable to be banned just because malicious actors use them.[31] Arguments and counter-arguments might vary, and analyses of the alleged use of cryptocurrencies in criminal activities and terror financing might lead to divergent conclusions, but certainly, cryptocurrencies have thrown open a whole new challenge towards which majority of the intelligence and law enforcement apparatus are inadequately prepared to tackle.

3. **Potential for Tax Evasion**: Cryptocurrencies are not regulated or controlled by governments, making them a lucrative option for tax evasion. Sales made or salaries paid in the form of cryptocurrencies could be used to avoid income tax liability. Taxation rules and regulations may vary from state to state, and many countries do not yet have policies in place for cryptocurrenices. There is, as yet, no agreement or understanding on whether the income earned through trading, or for that matter, even mining of cryptocurrencies, should be included in gross income or treated as capital gains. Some proponents of cryptocurrencies have gone to the extent of raising doubts over the authority of the state to enforce taxation on something they do not issue or have control on.[32]

---

28 Munish Sharma, "Triggers to Tabs: ISIS and the Information Age", in S D Muni and Vivek Chadha (eds.), *Asian Strategic Review 2016* (IDSA: New Delhi, 2016), available at http://www.idsa.in/system/files/book/book_ASR2016.pdf, p. 35, accessed on July 18, 2017.

29 Taqi'ul-Deen al-Munthir, "Bitcoin and the Charity of Violent Physical Struggle", available at https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf, accessed on July 18, 2017.

30 David Carlisle, "Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic", *Royal United Services Institute* (Commentary), March 2, 2017, available at https://rusi.org/commentary/cryptocurrencies-and-terrorist-financing-risk-hold-panic, accessed on July 18, 2017.

31 Anthony Mandelli, "Antonopoulos Answers the Inevitable Bitcoin-Terrorism Question", *CryptoCoin News*, May 21, 2017, available at https://www.cryptocoinsnews.com/antonopoulos-answers-inevitable-bitcoin-terrorism-question/, accessed on July 18, 2017.

32 Travis Patron, "Why Bitcoin Creates a Voluntary Tax System", *Coindesk*, September 7, 2015, available at http://www.coindesk.com/why-bitcoin-creates-a-voluntary-tax-system/, accessed on July 18, 2017.

Owing to the concerns regarding the perceived potential of cryptocurrencies for tax evasion, the Internal Revenue Service of the US Government had issued a notice in 2014, labelling them as "intangible property"[33]; and deemed trading in cryptocurrencies to be taxable;[34] and also clarified that digital currencies are capital assets and are therefore subject to capital gains taxes.[35] A similar debate over the categorisation of cryptocurrencies as security, currency or a commodity derivative is currently playing out in India.[36]

Cryptocurrencies do not have legal tender status in any jurisdiction, but many jurisdictions have already declared the transactions for the sale of goods or services, capital gains, income etc. as taxable. As taxation authorities are grappling with devising strategies and guidelines for tax compliance, tax evaders might find their tax havens in form of cryptocurrencies.

Cryptocurrencies in India: Opportunities, Risks and Policy Options

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

33 Rober A. Green, "If You Traded Bitcoin, You Should Report Capital Gains To The IRS", *Forbes*, February 21, 2017, available at https://www.forbes.com/sites/greatspeculations/2017/02/21/if-you-traded-bitcoin-you-should-report-capital-gains-to-the-irs/#3ce37bc3e3d8, accessed on July 18, 2017.

34 Craig W. Smalley, Cryptocurrency and taxes, The Tax Adviser, April 20, 2017, available at http://www.thetaxadviser.com/newsletters/2017/apr/cryptocurrency-taxes.html, accessed on July 20, 2017.

35 Tax Compliance, *bitcoinwiki*, available at https://en.bitcoin.it/wiki/Tax_compliance

36 Kevin Helms, "India Fights over Which Government Body will Regulate Bitcoin", *Bitcoin News*, July 23, 2017, available at https://news.bitcoin.com/india-government-body-regulate-bitcoin/, accessed on July 31, 2017.

37 n. 3.

38 Reserve Bank of India, "RBI cautions users of Virtual Currencies", February 01, 2017, available at https://rbi.org.in/scripts/bs_pressreleasedisplay.aspx?prid=39435, accessed on July 20, 2017.

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 platform[41], 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

---

39 Ibid.

40 Question (no. 234) by Smt. Wansuk Syiem in Rajysabha on recognising bitcoins for national economic growth, replied by Shri. Arjun Ram Meghwal (Minister of State in Finance), July 18, 2017.

41 Ibid.

42 Stan Higgins, "India Inches Closer to Developing Cryptocurrency Rules", *Coindesk*, June 20, 2017, available at http://www.coindesk.com/bitcoin-india-inches-closer-developing-cryptocurrency-rules/, accessed on July 20, 2017.

43 a) Question (no. 3931) by Smt. Meenakashi Lekhi in Loksabha on Bitcoin Exchange and Trading, March 20, 2015, available at http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=17078&lsno=16, accessed on July 20, 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.

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:

a) the thrust of the government towards Digital economy, driven by the flagship programs of the government for financial inclusion;

b) the risks of tax evasion, given the stringent regulations in the past one year for the crackdown on black and unaccounted money; and

c) the present security situation and experience with terrorism or Left Wing Extremism.

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

[44] Unocoin, "AML and KYC Policy", available at https://www.unocoin.com/post/106, also Zebpay, "Steps to Buy and Sell Bitcoins", available at https://www.zebpay.com/, accessed on July 20, 2017.

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.

[45] Jayanth Jacob, "India remains top remittance recipient with $6.2 billion earnings, but China closing in", *Hindustan Times*, may 05, 2017, available at http://www.hindustantimes.com/india-news/with-6-2-bn-wiped-off-remittances-to-india-experts-urge-govt-to-better-gulf-ties/story-3HYOtJaEqkECeDnOtf8UfL.html, accessed on July 20, 2017.

Factor	Risk	Regulated Environment	Unregulated/ Proscribed Environment	Risk Mitigation and Probable Policy Outcome
Liquidity and lower acceptability	Lack of liquidity deters genuine users from experimenting and hampers further growth.	a) Aid liquidity with authorised trading exchanges. b) Broadened acceptability with more awareness and rising business opportunities.	a) Black markets or unethical practices for trading in cryptocurrencies. b) Unable to extract the value proposition as alternate payment systems or electronic transfer of funds.	a) Authorised exchanges and trading platforms. b) Alternate payment system. c) Alternate mode for remittances.
Price volatility	Exposes the users to fluctuating costs, leading to losses.	a) Wider use for payments will possibly bring down volatility.	a) Infusion of unaccounted money and unfair trading practices will lead to price fluctuations.	a) Beyond the control of the government as the prices are driven by diverse factors. b) Wider user base and acceptability will stabilise the prices.
Consumer protection and dispute Settlement	Absence of governance mechanism exposes the users to the risks from frauds and there is no authority to mediate disputes.	a) Domestic laws can protect the rights of the users to an extent, inculcating trust and accountability.	a) State will not have control on any of the aspects of cryptocurrencies. b) Lack of trust or proscription will expose users to wider risks.	a) Domestic laws can protect the users. b) State will have limited jurisdiction as the architecture is decentralised and ledgers/parties are spread across the globe.

Potential use for Illicit Trade and Criminal Activities	Could be used for payments in the illicit trade of drugs, arms trafficking, ransomwares, money-laundering, cyber-crime.	a) Domestic laws can mandate the exchanges to report all suspicious trading transactions. b) Integration of exchange databases using APIs can aid law enforcement agencies.	a) State will not have control on any of the aspects of cryptocurrencies. b) The use of cryptocurrencies in such activities will remain unchecked.	a) Monitoring of trading transactions by law enforcement agencies. b) Unscrupulous/suspicious trading transactions to be reported to the authorities concerned.
Potential use for Terror Financing	Could be used as a means for anonymous funds transfer or to make donations, aiding terror financing.	a) Domestic laws can mandate the exchanges to report all suspicious trading transactions. b) Integration of exchange databases using APIs can aid law enforcement or intelligence agencies.	a) State will not have control on any of the aspects of cryptocurrencies. b) The use of cryptocurrencies in such activities will remain unchecked.	a) Monitoring of trading transactions by law enforcement agencies. b) Unscrupulous/suspicious trading transactions to be reported to the authorities concerned.
Potential for Tax Evasion	Could be used as a tool for tax evasion if the income and gains from business/trade is not disclosed voluntary.	a) Increase the reporting of sales and gains through compliance/declaration.	a) State will not have control on any of the aspects of cryptocurrencies. b) Proscribing will lead to loss of taxation or use of cryptocurrencies as tax havens.	a) Monitoring of trading transactions by Income tax authorities. b) Unscrupulous transactions to be reported to the Income tax authorities.

Key/Wallet/ Exchange Security	Security threats to the platforms as well as to the users, in form of theft, loss of keys, DDoS etc.	a) Mandate compliance to information and data security standards or practices. b) Motivate cryptocurrencies platforms for self-regulation and norms.	a) State will not have control on any of the aspects of cryptocurrencies.	a) Compliance with information and data security standards or practices. b) Adoption of norms/Self-regulation.
Anonymity/ Privacy Protection	By design, cryptocurrencies ensure anonymous transactions, preserving the identity of the transacting parties and the users.	a) Disclosure of identity might erode the underlying principle of anonymity on which cryptocurrencies are built upon. b) Disclosure of identity is possible at the time of trading only. However, identity of transacting parties is protected.	a) Anonymity and privacy of the users is protected.	a) Mandatory KYC norms, PAN Number, Adhaar for trading/sale/purchase at the authorised exchanges.

Cryptocurrencies in Regulated or Unregulated/Proscribed Environment: Risk Assessment

Low Risk
Moderate Risk
High Risk

About the Authors

Munish Sharma is Consultant at Institute for Defence Studies and Analyses, New Delhi.

The Institute for Defence Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
contact.idsa@nic.in www.idsa.in
Twitter @IDSAIndia
www.facebook.com/InstituteforDefenceStudiesAnalyses