Crypto-currencies demystified

1.0 Cryptography, per se, is quite old. Even Kautilya (Chanakya) in his administrative treatise "Arthashastra" speaks about cryptography in communication. He says that when a public carrier or a messenger takes a message from one king or a head to another minister or a king or some such critical authority, he should be given the communication in such a way that he carries the message and even if he or anyone else reads the same en route, he/she should not be able to understand the content. This is what exactly cryptography and encoding a message is. And this is what global IT giants like Facebook (who owns WhatsApp) say when they claim that the messages are end-to-end encrypted.

1.1 To define, Cryptocurrency is a currency always maintained in a crypto format ie no one other than the intended persons, can understand or decipher what it is.

1.2 **What is cryptocurrency?** The world is now witnessing a new form of currency, viz. cryptocurrency. It can be loosely equated to digital currency, although it is not exactly synonymous. In the organised and regulated market, there is always a systemic representation of the digital form of currency (as opposed to physical currency). A physical and conventional currency is a coin or a printed note like US dollar, Indian Rupee or the Pound Sterling etc, all of which we can see, carry and use. As against this, a bitcoin is a virtual currency as accepted modes of payment and currencies of exchanges in the limited group within which they are traded, at the market determined (though highly volatile) rate.

1.3 **Is it a currency?** In any economy, besides the physical currency notes in circulation, substantial exchange is also done through banking transactions i.e. in digital and non-cash and non-physical or electronic format, which represent a major part of the nation's economy. From this perspective, crypto-currency DOES NOT REPRESENT THIS quantifiable, measurable, accounted and physical figure, since it is never reported to the regulatory authority like the RBI in India, nor even recorded in any bank. Crypto-currency can be loosely called a virtual currency, though there are some technological and legal differences between these two, as stated above. Virtual currency may be even taken to mean the balance in the accounts of individuals or firms in any banks which can become a physical currency at any time. A crypto currency can NEVER take a printed form, because it is NOT monitored, NOT regulated and nobody has given any shape or colour or design or model to it and hence it can NEVER be printed or SEEN.

2.0 **What is Bitcoin?** Bitcoin is a crypto-currency, (like there are many other crypto-currencies eg Etherium,) a digital asset, and a payment system owned by nobody, regulated by none, and expressed as an open computer source software. It is accepted as a means of payment by a particular group of people. Bitcoins is considered to be the earliest of crypto-currencies, though many other such currencies have now flooded the market, at present worldwide, the number is around 1500.

2.1 **Genesis of Bitcoins:** It was reportedly invented in 2009 by a Russian named Santoshi Nakamoto, whose biography is mysterious and not much is known about him (or maybe a group of men by that name, who could be the founders) for reasons better known to him/them. Till date, there is confusion whether such a person ever existed or it is a just a creation or a pseudonym to one or more men who originally created the software and the group to trade. There have been attempts to 'discover' the history of this founder, known as Santoshi. No fruitful results so far. While introducing the concept of Bitcoin, the unknown person or people also introduced the first database for the technology called Blockchain, to enable payment through Bitcoin. In this crypto-currency, it is just the computer system software i.e. the cryptographic source code that 'shows' the balance or 'evidences' the currency balance. Bitcoin is a cryptographically secure medium of financial exchange and not a 'fraud' though it comes under 'unregulated' medium. Bitcoin is basically 'digital' without a physical form.

RBI's stand is presented in detail in the later part of this story.

If you want to read only about crypto-currenies like Bitcoins and skip the technology part, go to para No.4.0

3.0 **Technology behind cryotocurrencies** is normally a blockchain technology. Blockchain is a public distributed ledger verified by network nodes and authenticated through the computer source code in the app provided. It is an open source software, with no person, company or country owning this network, **just as no one owns the Internet.** In this system, users transact directly with the other end, without an intermediary like a bank or a credit card company or a clearing house. Since this is a computer based cryptographic technology, it has become easier in the modern day digital banking era, for many banking transactions too. Some private banks in India are reportedly transacting through blockchain already.

3.1 Blockchain technology is prophesied to change the world, portended to rock the banking industry and revolutionise its basic structure, just as the internet did, a few decades ago, in changing the way the world communicates. Blockchain technology is defined as a digitised and decentralised public ledger of all crypto-currency transactions. It is a system on which virtual currencies like Bitcoins and Ethereums actually sit. A blockchain can be compared to the Operating System (like MS Windows or Mac etc) of a computer, on which applications like Browser and Office Suite with MS Word etc are loaded, and function. It is like a public ledger in which the participants maintain accounts in the form of virtual currency or crypto-currency called Bitcoins or Ethereums and was originally developed as an accounting method exclusively for such currencies, but in a short span of a few years, this technology has progressed greater compared to that of Bitcoins, for which it was conceptualised.

3.2 Blockchains have been growing at such a pace that observers say, it is going to re-write history in the global e-commerce arena. Since a blockchain is maintained in a digitised and decentralised format, it is perceived to be tamper evident, and maintained in an immutable manner. It reduces the friction among the various participants in commerce, traces the product and keeps track of it at every stage as a block. For instance, when you buy a car, many parties and lots of contractual obligations are involved in several stages, like the manufacturer's ledger (books) with the progress recorded therein, the dealer or the wholesaler's ledgers, the financier's books (like banks or other lenders, if any), the registration authorities and then the ultimate consumer's ledgers.

3.3 In a blockchain, the manufacturer, as a participant, marks the models being manufactured and other details. The dealer thus gets to know the number of vehicles available, with complete details. The regulatory government authorities mark the same with details for registration and numbering purposes and the financier or the leasing company marks the same as part of the contractual obligation between the lessor and the lessee. The ultimate consumer or user has all these details by the time the vehicle is delivered to him.

3.4 From the above example, it is evident that blockchain stores the transaction data in blocks in such a way that each block is linked to the next and the entire process is completely transparent and tamperproof. Each block leads to the next and the sequence is maintained, preventing any ad hoc insertion or alteration. Each participant in the chain is like a

node in a network, accessing through a hash algorithm (ie converting a data of varying and arbitrary sizes into a fixed size and encoding it in a specific programme-driven manner) in a secure manner with a user ID and password, with a copy of the blockchain downloaded automatically.

3.5 **Application of Blockchain Technology:** In conventional commerce, ledgers are traditionally and typically maintained at every entity, ie. at every participant's level, whereas in a blockchain there is a common ledger through which the transaction flows across all the stake holders, enabling all the participants to view the entire process-flow. It is distinct from a database and hence can be linked to any database including banking. Blockchain can be compared to a SWIFT (Society for Worldwide Interbank Financial Telecommunication) transaction that enables trade payment among all member banks throughout the world accepted globally as the most popular one, ensuring security of communication. It is generally a stand-alone package that should be systemically or manually integrated with the Core Banking Solution of any bank that maintains the accounts of its customers.

3.6 It is **by itself a distinct technology and database** and thus, not a replacement of databases, or a messaging technology, but attached to the banks' or other firms' databases as a supplement. That is why it is said that some banks across the world have already started using the blockchain technology or money transfers (presumably attaching the data into their own core banking based databases or their in-house data structures). However, some people say that blockchain may eventually even replace the banking services or at least reduce its dependence to some extent, with many transactions going across through this technology as inter-party, in an e-commerce transaction, and the various contracts, various sets of bi-polar or two-party contracting parties at every stage getting replaced with a single smart contract in this block.

3.7 **There are various parties to a blockchain.** The user is a participant who conducts the transaction and is not directly concerned with the technology (like a customer of a bank is unmindful of the technology in the bank). The regulator has special permission to oversee the transaction and does not conduct any transaction, whereas the network operator has permissions to create, define and monitor the network (like the Database Administrator in a Core Banking Data Centre). Programmers and developers enable traditional data transfer from existing databases of legacy firms and participants to the block through an electronic data interface, data exchange and other data transfer

modalities. In India, recently in an interbank interactive survey, it transpired that 13% of the banks were already in production implementation of blockchain technology, while 30% were in the Proof of Concept stage with blockchain provider firms; 44% in the stage of formulating a strategy and evaluation, and the remaining 13% were 'looking into the technology'. This is perhaps an indicator that the blockchain technology has come to stay in India. '*BankChain'* is reported to be India's first Blockchain exploration consortium launched by the public sector giant State Bank of India in February 2017, with more than 30 banks including public sector, private sector and foreign banks and institutions like NBFCs, National Payment Corporation of India etc, as members, in partnership with Microsoft, IBM, Data Security Council of India for expertise in their respective areas.

4.0 **How to open a Bitcoin account?** To open a Bitcoin account (or any crypto-currency), you have to log in to the particular website (of the agent or the exchange), have a username created along with a password, and then have the initial money transferred from your regular bank account or even an e-wallet like PayTM. These accounts are normally opened with zero balances also. At the time of opening of a Bitcoin account, the firms claim that they do ask for identification credentials like passport or Aadhaar and add that these details are not shared with any one and the id is never revealed. Being completely non-regulated, there is no fear of these id details being given to the government or regulator like RBI, SEBI or TRAI. It is also reported that subsequently the details so given may always be altered with no further submission of id proofs. Needless to say, with a court order the id has to be shared in accordance with the order.

4.1 **This anonymity the greatest feature** of a Bitcoin account. The account holder is always identified with his number and there is no hint even about his name, age or nationality or any such detail about the account holder. You can give this account number (normally around 25 digits), to the parties and request them to pay to this account in this exchange itself, thereby converting your USD or INR to this exchange-currency. You can later view in this ledger and trade in this exchange further, depending on that particular day's rate value, and, to be precise, the rate value at that particular time.

4.2 There are many European nations, mostly the smaller ones, like **Slovenia, Estonia, Switzerland** (which has one of the biggest Bitcoin exchange houses by name 'Coinbase;), **Luxenberg** (which has 'Bitstamp'

one of the most popular Bitcoin exchanges), in which many crypto-currencies especially the Bitcoins are freely traded and widely accepted. It is widely reported in business circles not just in the grey market or the darkweb but in the open Internet too, that many businessmen and politicians invest in these nations and crypto-currencies, through which their account balances are not regulated, not transparent with even the names not revealed but exchange (ie buy and sell or transfer to and receive from) takes place with absolute comfort by the click of a mouse in the computer. 'Bitcointicker' and similar other websites show the volume of trade in Bitcoins every second and live Internet streaming is always on and it is quite amazing to see the volume of trade that takes place there.

4.3 **Bitcoin's rivals:** Bitcoin is not a monopoly. Although it was the number one crypto-currency, other such currencies also functioning on the blockchain technology, are now catching on. Bitcoin, which once enjoyed more than 80% of the market share, has now reportedly come down to less than 50% market share. There are many other rivals like Ethereum, Ripple and Litecoin which are also accepted with reasonably wide recognition among specific groups and industries. There are frequent comparisons in the Internet on the ease, acceptability, security, dependability and popularity of various crypto-currencies.

5.0 **Ministerial Committee:** There was a Ministerial Committee on Victual Currencies which submitted its report on 28 Feb 2019, suggesting specific actions, from a national perspective, with the Secretaries from the Dept of Economic Affairs, Ministry of Electronics and IT and Chairman, of SEBI and the Deputy Governor of RBI. The Committee recognised and placed on record the importance and the emerging significance of the Distributed Ledger Technology (Blockchain technology) and recommended that it can be deployed in specific domains requiring maintenance of customer database and a common data of KYC and such information. It even presented a draft bill to regulate the use of this technology especially in the financial and related sectors.

5.1 On the use of crypto-currencies, the Committee stated that crypto-currencies cannot serve the purpose of a currency. The private crypto-currencies are inconsistent with the essential functions of money/currency, hence private crypto-currencies cannot replace fiat currencies adding that private crypto-currencies have not been recognised as a LEGAL TENDER in any jurisdiction. The Committee recommended banning all private crypto-currencies in India and endorsed the stand taken by RBI to eliminate the interface of institutions regulated by the RBI

from crypto-currencies, prohibiting all exchanges, people and traders from dealing with crypto-currencies. It recommended a law banning the crypto-currencies in India.

This committee report has been referred by the Hon'ble Supreme Court in the judgement cited below.

6,0 **Role of RBI, the regulator:** Crypto-currency called by any name and of any origin, is not officially recognised in India by the financial regulator, RBI. Anyone trading in Bitcoins or other such crypto-currencies would be doing so, completely at his own risk, playing in a field where there is no referee, no umpire, no intermediary and no rules and regulations. Even then, notwithstanding this uncertainty, the use of crypto-currencies especially Bitcoins is on the rise and the volume of trade is increasing, especially among the high-stake financial players with an appetite for risk. It is said that although it is not recognised at present, the underlying technology behind crypto-currencies will continue to exist. With a view to discourage the use of Bitcoins, the Finance Ministry has even labelled it as a worthless Ponzi Scheme.

6.1 RBI, the national regulator issued a ***"Statement on Developmental and Regulatory Policies"*** on April 5, 2018, paragraph 13 of which directed the entities regulated by RBI (i) not to deal with or provide services to any individual or business entities dealing with or settling virtual currencies and (ii) to exit the relationship, if they already have one, with such individuals/ business entities, dealing with or settling virtual currencies (VCs). Following this, RBI also issued a circular dated April 6, 2018, in exercise of its regulatory, controlling and monitoring powers, directing the entities regulated by RBI (ie banks and financial institutions on both the points cited above.

7.0 **The Legal Position:** This circular of RBI was challenged, in ***Writ Petition (Civil) No.373 of 2018 in*** the **Supreme Court,** by an industry body 'Internet and Mobile Association of India'. Delivering a 180-page detailed judgment, V. Ramasubramanian, J, along with R.F. Nariman J, and Anirudha Bose, J. allowed the writ petition and held that the petitioners are entitled to succeed and the impugned RBI Circular dated 06-04-2018 is liable to be set aside on the ground of proportionality. Calling the last operative part of the judgment as "Climax", the judgement gave many interesting analyses, appreciated the regulatory role of RBI, though with a surprise last para struck down the circular as excessive in proportionality.

7.1 The Statement of RBI, referred to above, dated 05-04-2018, though

challenged in one writ petition, was also held to be not in the nature of a statutory direction. In the para, the judgement said that "While we have recognized elsewhere in this order, the power of RBI to take a pre-emptive action, we are testing in this part of the order the proportionality of such measure, for the determination of which RBI needs to show at least some semblance of any damage suffered by its regulated entities. But there is none. When the consistent stand of RBI is that they have not banned VCs and when the Government of India is unable to take a call despite several committees coming up with several proposals including two draft bills, both of which advocated exactly opposite positions, it is not possible for us to hold that the impugned measure is proportionate."

7.2 We can understand that the Hon'ble Supreme Court felt that the circular issued by RBI is not 'proportionate' to the powers vested with it and the stand of RBI has not been made clear and no damages or ill-effects of crypto-currencies have so far been felt. Interestingly, the Hon'ble Supreme Court felt that RBI can take steps like banning the crypoto-currencies etc , AFTER the damage is felt or the adverse impact actually materialises.

7.3 It is pertinent to note that in para 6.173, the Hon'ble Supreme Court states Quote

> It is no doubt true that RBI has very wide powers not only in view of the statutory scheme of the 3 enactments indicated earlier, but also in view of the special place and role that it has in the economy of the country. These powers can be exercised both in the form of preventive as well as curative measures. But the availability of power is different from the manner and extent to which it can be exercised. While we have recognized elsewhere in this order, the power of RBI to take a pre-emptive action, we are testing in this part of the order the proportionality of such measure, for the determination of which RBI needs to show at least some semblance of any damage suffered by its regulated entities. But there is none. When the consistent stand of RBI is that they have not banned VCs and when the Government of India is unable to take a call despite several committees coming up with several proposals…." UNQUOTE

7.4 Discussing the question of proportionality of the RBI's exercise of powers, the Hon'ble S.C. struck down the RBI circular and permitted the use of crypto-currencies. Now, encouraged by this judgement, which many interested firms and individuals interpreted as the S.C.'s approval of cryptocurrencies like Bitcoins, there is a mushrooming growth on the use of crypto-currencies and open advertisements for Bitcoin accounts and transactions based on this.

8.0 If the Bitcoins or any crypto-currency for that matter, is to be called a 'currency' it comes under the purview of RBI as the regulator of all

currencies in India and it is well within the powers to ban or permit or regulate or take an appropriate action. If it is not called a 'currency' which actually it is not, then we can call it an electronic document and in such a case, electronic documents are recognised in India as per the Information Technology Act 2000 and its Amendment Act 2008, and the express exceptions in the Act like 'will', 'negotiable instrument' etc do not include a crypto-currency as an express exclusion. Hence to regulate the same or to ban it, the Ministry of Electronics and Information Technology Dept may have to step in. Being un-regulated, it is a perfect haven for black money. It may destabilise the financial structure of the nation, in the long run. It is a perfect tool for money laundering. Many payments for ransomware attacks like *'Wannacry', 'Cryptolocker', 'Jigsaw', 'Aids Trojan'* etc (use of a malicious software that locks the computer system or completely denies access to the data inside, until some huge ransom money is paid) are always demanded in such crypto-currencies only, so that the receiver's identify is not known and the entire transaction is un-regulated, non-traceable and non-monitored.

8.1 **One simple example** about the use of Bitcoins and crypto-currencies in general is the use of some paper tokens or plastic coins used in a particular campus say an IIT or an Anna University which has a canteen, a few petty shops, a few pan shop, some stationery stores etc all within the same campus. Suppose the canteen uses a plastic token currency in various denominations and returns the same to students as the balance after a purchase and suppose further the same tokens are freely exchanged inside the campus ie in all the shops inside the campus as stated above. In a small measure and within the campus it may be acceptable but when it becomes a freely traded money outside the campus and in a major proportion, this becomes a 'currency' beyond the purview of financial structure of the nation and RBI in particular and is certainly illegal. Extrapolate and elongate this to a wider area and this becomes a wholly un-regulated and unmonitored but freely accepted market, the usage, depth and dimensions of which will not be measurable. This is what is Bitcoins kinds of crypto-currency, today.

9.0 **The case against** crypto-currencies: (Frankly, it was even said that these points were not properly highlighted by the government or the RBI in the case filed in the Supreme Court), RBI or the Ministry have not gone for an appeal or a review petition against the S.C. verdict cited above presumably because they are not quite serious about banning this. Banning is well within the law-making powers of the government, but still no such law is being proposed or not reported to be in the making.

9.1 Bitcoin is a perfect black money, since the money transferred to this account neither reveals the transferor to the transferee nor the transferee's details to the transferor. This anonymity makes it the perfect haven for black money or illicitly acquired money and to convert it into

any crypto-currency as well as from one crypto-currency to another and to any other legal currency ie money laundering activities. This is a perfect tool for giving or taking bribery and enhance the level of corruption of huge amounts in high places in payments running into crores with no involvement of banking transactions.

10.0 **Global Scenario**: Nations worldwide have not yet taken a clear stand on the use of crypto-currencies. Understandably, it is feared that an unregulated and volatile system of payments and settlements has all the potential to destabilise any economy and derail the financial progress of the nation. Some nations have banned crypto-currencies and called them illegal, while some have recognised it, while a few countries have not specifically banned it or called it illegal but recognised the underlying technology of blockchains for transfer of funds. It is legal in countries like USA, Mexico, Canada, Brazil, Japan and Singapore, while countries like China and Russia have not recognised it as public currency.

10.1 **High Value and Volatility:** Today, the rate of a Bitcoin is around Rs.7.3 lakhs per bit coin (unit). Since it is so costly, as compared to INR (Indian Rupee), trade in India vis a vis BTC (Bitcoins) is always done as a fourth or a fifth decimal, because as on date, even one thousand rupees equals 0.0014 BTC only. It is volatile, unpredictable, uncontrolled and completely unregulated not coming under any particular nation's regulatory mechanism. Some countries have not even recognised this as a currency (though many software and IT giants worldwide including Wiki, Google etc have approved and reportedly receive payments in Bitcoins). The currency is so volatile that its price fell from USD 19,000 on 16th December 2017 to a low of USD 12,000 on 30th December 2017. Perhaps it is this volatility that makes it interesting to many, and irresistible to those with a risk appetite.

10.2 In today's international trade, Bitcoin is the one with the highest value, a rate that is unimaginable, with even Google recognising it as a currency, and displaying its value in its normal searches. Already, some 175 million US dollars' worth of crypto-currencies are reported to be 'stolen' as a result of hacking into the servers of just three exchanges so far. The exact figure remains unknown. With such a huge unregulated market, unmonitored transactions and intermediary-less opaque deals, where would one report these cyber-crimes? Since the value of crypto-currencies is soaring, hackers consider it as easy-target-more-money than the conventional and normal electronic banking sites.

The Future There are diverse opinions about the use, and the future of Bitcoins. Some people (frankly, very few) say that it is the future currency of the globe, though serious and learned economists are quite sceptical about the use of cryptocurrencies. The well-known American business magnate and philanthropist, Warren Buffet arguably among the most successful investors of the world, has gone on record saying that cryptocurrencies have a bad ending and his firm was not interested in it. And recently, according to Forbes' latest list of billionaires, Satoshi Nakamoto, Bitcoin's mysterious inventor/s (where is he now?), is among the world's 50 richest people. There are many corporates across the globe accepting or in the process of accepting Bitcoins as a medium of payment.

11.0 **In India** too, as a first of its kind, some leading software giants have developed and are using the Blockchain technology, on which Bitcoins trading is done (and maybe other crypto-currencies too). Reliance Jio is now reportedly planning its own cryptocurrency to be called 'Jiocoin' and a young team of finance and software professionals is working to launch it soon. If a few more companies join the bandwagon, it would be interesting to watch what stand our regulator, RBI will take to deal with the issue. As of now, the Finance Ministry has cautioned about the risk associated with these digital currencies and warned that they may become a tool for money laundering and other clandestine payments.

11.1 **Some incredible but interesting titbits**: It is reported that just 1% or 2% of the Bitcoin community controls more than 90% of the Bitcoin wealth and only less than 1000 people worldwide, own half of all Bitcoins. Ethereum, a popular cryptocurrency, saw an incredible increase of around 40 times, in just 5 months i.e. from USD 5,000 to USD 199,400. Communication among the groups is mostly encoded and not easily accessible in the Internet.

12. **To conclude,** with everything becoming digitised (moving away from physical), it would be interesting to watch the progress of such cryptocurrencies. It would perhaps be like watching a performance from the gallery. Wisdom has to prevail upon the users to stay away from such unregulated, unmonitored market. Any concerned government, sincerely worried about the use of black money or corruption, will enable its regulator to ban or at least evolve means to monitor and control the wide usage of crypto-currencies.

****.****