SUPREMO AMICUS

VOLUME 16 ISSN 2456-9704

BLOCKCHAIN, CRYPTOCURRENCY: IS STATE REGULATION NECESSARY?

By Kezia Rasmi Jude
From Christ (deemed to be) University, Bangalore

ABSTRACT

Cryptocurrencies like bitcoin and Ethereum are decentralized, digital currencies relying on a peer-to-peer network which operates without the need for a third-party intermediary. Coupled with the lack of regulatory guidelines and its unique technical aspects create huge complications as well as more scope for research. The blockchain concept reflects the changing views and ideologies of society in terms of systems established on the basis of trust, especially the legal system. With the rise in market for use of cryptocurrencies throughout the world in the recent years, it is imperative to understand how blockchains work, their technology and future. Part A of this article begins with an introduction to blockchains which have heterogeneous and technical characteristics. The article goes on to explain the various costs and risks involved in transacting with cryptocurrencies. Part B of this article deals with the Howey test, and the current regulatory mechanism prevalent in the US and in India and best practices for cryptofunds.

PART A

BACKGROUND

Crypto currencies are created through a process called 'mining' which is characteristically a mathematical process, i.e., hash function. A 'miner' who has particular hardware processes the transaction. With every next set, it keeps getting difficult to solve and hence it's supply is assumed to be constant. From an economics point of view, in the recent times, we see that the supply remains constant and there is a rise in demand which causes the price to keep increasing.

By solving the hash function, i.e., solving the puzzle, the node that receives the transaction authenticates it. Each network of nodes (computers) receives a certain amount of crypto currencies as a reward for authenticating. A 'ledger' is maintained to keep a record of each transaction and it can be of two types: centralized or decentralized. Centralized is when there is a single party who controls the database and software is run by him. Decentralized is when there is no single party and multiple nodes run the software. Once the transaction is verified, a 'blockchain' is formed. Blockchain is created when a block is added to the chain after verification by thousands of computers and is stored as a unique record. Each block contains a hash function, data of the previous block and transaction data. To falsify a single record would mean to falsify the entire chain of instances, which is near to impossible. Bitcoins work on proof- of-work basis where puzzle is solved and the property rights are assigned by that person who solves it first in the new block. Thus, in a decentralized setup, increase in capital investment can be helpful in acquiring control. [1]

Once a bitcoin is formed, it can be traded for regular currency prevailing in the current

[1] Kevin Werbach, Trust, but Verify: Why the Blockchain Needs the Law, 33 Berkeley Tech. L.J. 487 (2018).

market exchange rate and the money is transferred to the purchaser's wallet which has two keys. A private key is used to decode the bitcoins transferred to the wallet of the recipient. Private key remains only with the recipients. The payer can use his public key to encode payments. A 'fork' can be installed which can create modifications to the software. When a blockchain is "diverged into two paths forward" it is called a fork. It can be hard fork which means the software validating according to the old rules will render the news as invalid. Soft fork on the other hand, would be recognized as valid though there is change in rules. Thus, fork can either improve or upgrade the existing one or it could be to create a rival blockchain.

Hence, blockchain technology works by :(1) The means of creating virtual assets- "tokens," or "cryptocurrencies"-and assigning such assets an underlying value implemented through code, contract (2) A quantitative methodology for allocating ownership in these virtual assets and representing it publicly on a ledger (3) A platform for trade in these virtual assets, in exchange for Bitcoins, Ether (ETH), or other cryptocurrencies, all easily exchangeable for U.S. dollars (USD) and other major international currencies on the internet. The value of the blockchain is represented by the intrinsic value of the block itself, i.e., the technological merit or the size of the users of the blockchain. It can also be valued based on the underlying assets which are dependent on performance of goods or services in the entrepreneurial sector.

Tokens are placed in the public domain through an Initial Coin Offering (ICO) which is similar to the initial public offering, IPO in the traditional market. The key difference between the crypto market as compared to the traditional one is that, in the traditional market, that is the IPO the number of units (shares) being offered to the public are specified whereas in the crypto market, the unit size keeps growing as mining process constantly and continuously keeps occurring . In the crypto market there is no underwriter, credit rating, intermediaries and the transaction is carried out through a 'smart contract'. The legally binding contract of the blockchain is given in its code which is the software. It is not easily comprehendible to the layman as it requires technical knowledge of programming and hence companies create a 'white paper' to provide details about the offering. The white paper makes the functioning of the blockchain understandable to the common man by limiting the use of technical jargons. This is a part of their marketing initiatives and is in English. However, it is often noted that there are significant differences between the code of the blockchain and the white paper offered to the public.

THE IDEA OF TRUST IN CRYPTOCURRENCY

Let us consider the examples of Bitcoin and Ethereum.

- Bitcoins were created by Satoshi Nakamoto who released a white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008 and implemented the same software.[2] The concept of trust is not present as there is there is no institution like a centralized bank to regulate. This also gives rise to the problem

[2] S Nakamoto,"Bitcoin: A Peer to Peer Electronic Cash System" (2008) available at http://nakamotoinstiute.org/bitcoin/

of *double spending* where it is hard to prevent people from spending the same digital cash twice. To tackle the issue of trust, bitcoins follow the *proof of work* approach which involves solving a mathematical algorithm function within a specified amount of time. *Timestamp server* is another way to tackle this issue by "taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper of Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get the hash."

- Ethereum is another blockchain and the cryptocurrency is Ether. It deals with a concept wider than trust- the problem of having an agency to regulate the blockchain. In order to make it decentralized, etherum works based on '*smart contracts'* which has programmed rules as to how the block will function. However, in 2016, DAO- Decentralized Autonomous Organization faced a loss of $50 million due to hack in the 'smart contract' which had an error. Since such a contract is a "one-way train", the only way to remedy this was to create a 'fork', thereby splitting into Ethereum Classic- the original Ethereum blockchain that continues to run alongside the fork, Ethereum Hard Fork (ETH) created. [3]

COSTS AND RISKS INVOLVED

- Controlling costs: Controlling occurs when a person significantly influences the blockchain and its operation. In a decentralized setup of blockchain, it is not possible for a single party to have control as there is no intermediary. However, in reality, the controlling costs occurs on various degrees and is based upon any party exerts any control, whether such control involves cost, i.e, diverting cryptocurrency to himself or agent, and whether ultimately, this leads to an abuse of the other token holders.
- Monitoring costs: An ex- ante evaluation of the merit of the investment and an ex- post evaluation of its performance is involved in monitoring costs. An on-chain blockchain does not involve monitoring costs as it has automated verification. When the token is dependent on underlying assets or technologies which are subject to future market transactions are called off-chain transactions. Such transactions require high monitoring costs as they are prone to manipulations.
- Technological risk: Blockchain is exposed to risks of bugs, manipulation, coding mistakes and cyber-attacks. Unlike traditional contracts, bitcoin contract cannot be altered as they are to a large extent immutable. They do not have ex-post remedy of approaching the court.
- Systemic risk: Blockchains involve technical jargons which a common investor will not be able to process at ease and hence there is a lack of well-informed investors. Another systemic risk is with regards to 'forks' being created with new currency being created on top of original blockchain stakeholders. The third risk is related to the 'stickiness' of the contracts, i.e., rigidity of the contracts which makes it extremely difficult to alter. [4]

PART B

WHETHER THESE ARE INVESTMENT CONTRACTS? - HOWEY TEST

[3] Alan Cunningham, Decentralization, Distrust & Fear of the Body - The Worrying Rise of Crypto-Law, 13 SCRIPTed 235 (2016).

[4] Shlomit Azgad-Tromer, Crypto Securities: On the Risks of Investments in Blockchain-Based Assets and the Dilemmas of Securities Regulation, 68 Am. U. L. Rev. 69 (2018).

Under Sec 2(1) of the Securities Act, 1993 of the US defines securities and it includes 'investment contracts'. SEC v WJ Howey Co.[5] is the case that laid down the test for whether a particular transaction can be classified as an investment contract. The test is four-fold: (1) investment of money (later interpreted to include other considerations as well) (2) in a common enterprise (3) with an "expectation of profits" (4) with the efforts of others. There are three ways through which court can determine whether the investment is in a common enterprise. Under horizontal commonality, unlike stock of a company, bitcoin fund is not polled together into one entity. However, though there is no pooling of funds, the investors share the risks and rewards of their investments. Vertical commonality is not satisfied as there is no "direct correlation between the promoter's success or failure and the investors' profits or losses." Finally, the broad vertical commonality is also not satisfied as the investors of bitcoins contracts do not rely upon the promoter's managerial proficiency and efforts. In addition to this, the profits are not dependent upon the efforts of others as the ability to mine, control and sell one's own coins remains with the investor itself. Hence, bitcoins do not satisfy the Howey test.

No comprehensive federal regulation exists for virtual currencies. [6] Securities law and other forms of regulations in the cryptocurrency regime are subject to international law and policy theory. There would be a conjuncture globalization and state laws, free markets and regulation and capitalism and anarchy. The questions over extraterritorial jurisdiction of states also come into question. The justification for applying securities laws to blockchains would be that it ensures mandatory disclosures thereby protecting the vulnerable investors by removing information asymmetry between them and the offerors. It ensures standardization and provides a benchmark based upon which investors can make decisions rather than just providing raw data. Corporate governance and transparent system is one of the other benefits of regulation.

This makes policy-making to reach a conflicting position. On one hand there is investor protection which is the prime aim of securities laws and on the other, the risk of limiting innovation and technological advancements which thereby hinders the growth of start-ups that use bitcoins for raising capital, through tedious disclosure and registration requirements. [7] Cryptocurrencies pose political constraints as by making it subject to regulations made by the Securities Exchange Commission (SEC) [a regulatory body in USA enforcing securities laws] the very core of the blockchain system which is to detach the intervention of states and regulators, is lost. SEC would ultimately extend its reach to ascertain power over these private markets as well.

CURRENT REGULATORY MECHANISM IN INDIA

Though at present, there is no regulatory framework governing bitcoins it has not been declared to be illegal to be transacting with them. The Serious Fraud Investigating Office

[5] SEC v. W.J. Howey Co., 328 U.S. 293, 297 (1946).

[6] Trevor I. Kiviat, Beyond Bitcoin: Issues in Regulating Blockchain Transactions, 65 Duke L.J. 569 (2015)

[7] Justin Henning, The Howey Test: Are Crypto - Assets Investment Contracts , 27 U. Miami Bus. L. Rev. 51 (2018).

(SFIO) under the Ministry of Corporate Affairs has been directed to collect data regarding the use of bitcoins in corporate entities. The versatile nature of cryptocurrencies leads to a difficulty in classifying it into a computer programme or a security or derivatives or, goods and services, or a currency. If it is to be classified as a good or service it would be drawing tax implications under the relevant GST Acts. If it were to be treated as a currency it has to satisfy the criteria as given in the Foreign Exchange and Management Act (FEMA), 1999. Foreign currency must satisfy the definition as laid in the RBI Act and it must be legally accepted as unit of account in some other country. If bitcoins are to be classified as currency, then there would not be any tax implications. Furthermore, as cryptocurrencies are expressed in codes providing a scope of interpreting them as computer programmes thereby making them eligible for protection under the Copyrights Act, 1957.

The traditional securities market as regulated by SEBI is extremely volatile in nature. Similarly the volatile nature of cryptocurrencies gives an impression that they are securities or derivatives. Sec. 2(h) of Securities Contracts and Regulations Act (SCRA), 1955 defines securities. The central idea is that it must be issued by an 'issuer'. Cryptocurrency, on the other hand, is not issued by any authority, hence is decentralized. Thus unless it is issued by Central government, cryptocurrency will not fall within the ambit of the definition of securities. Derivative is a contract to hedge risk and derives its value from an underlying asset. It does not hold an independent value. Cryptocurrency is not a contract per se and are independent in nature. Hence, they are not covered under the definition of derivative as well.[8]

Various contracts and consumer laws are not sufficient enough to encompass the needs of the issues arising out of misuse of cryptocurrency. The remedies offered by contract laws such as damages, restitution, specific performance, rescission will not be wide enough to mitigate the damage caused. Consumer welfare legislations provide ex-post remedy by making a representation in courts. Moreover, courts are institutionally ill- equipped with the relevant technical knowledge about blockchains and cryptocurrency.

In order to bypass securities laws regulation and rather than being termed as an investor, issuers concentrated on channelizing purchaser motivation to that of consumers who are only protected by contractual rights. Returns are distributed in assets and are popularized by websites. The open platform for discussion among the crowd ensures that only accredited investors may invest and there is a cap on the maximum amount that can be raised. Some precautions must be taken by investors such as never transmitting the keys electronically through email, upload, etc. Managing keys with a secure electronic wallet and limiting trading authorization are some other methods to ensure investor protection. [9]

CONCLUSION

[8] Hatim Hussain, Reinventing Regulation: The Curious Case of Taxation of Cryptocurrencies in India, 10 NUJS L. Rev. 792 (2017)

[9] Edmund Mokhtarian & Alexander Lindgren, Rise of the Crypto Hedge Fund: Operational Issues and Best Practices for an Emergent Investment Industry, 23 Stan. J.L. Bus. & Fin. 112 (2018)

With the huge uncertainty lurking around use of cryptocurrency, the legislators and courts all around the world have a unique policy decision to make. The challenges faced to render it beyond scope of securities regulation and the risks involved in investing in cryptocurrencies have been discussed. There is a need for India to decipher the nature of cryptocurrency and classify it into a security, currency or commodity or any other definition in order to decide upon the tax implications of the same.

The thin line between adequately regulating this market and ensuring a decentralized platform must be constantly balanced. Another delicate issue which must be considered by regulators is hindering the growth of entrepreneurs who could raise capital at ease by using cryptocurrency. The current public enthrallment and increasing demand, regulators are bound to tailor the scope of regulation appropriately with the risks in mind.

*****