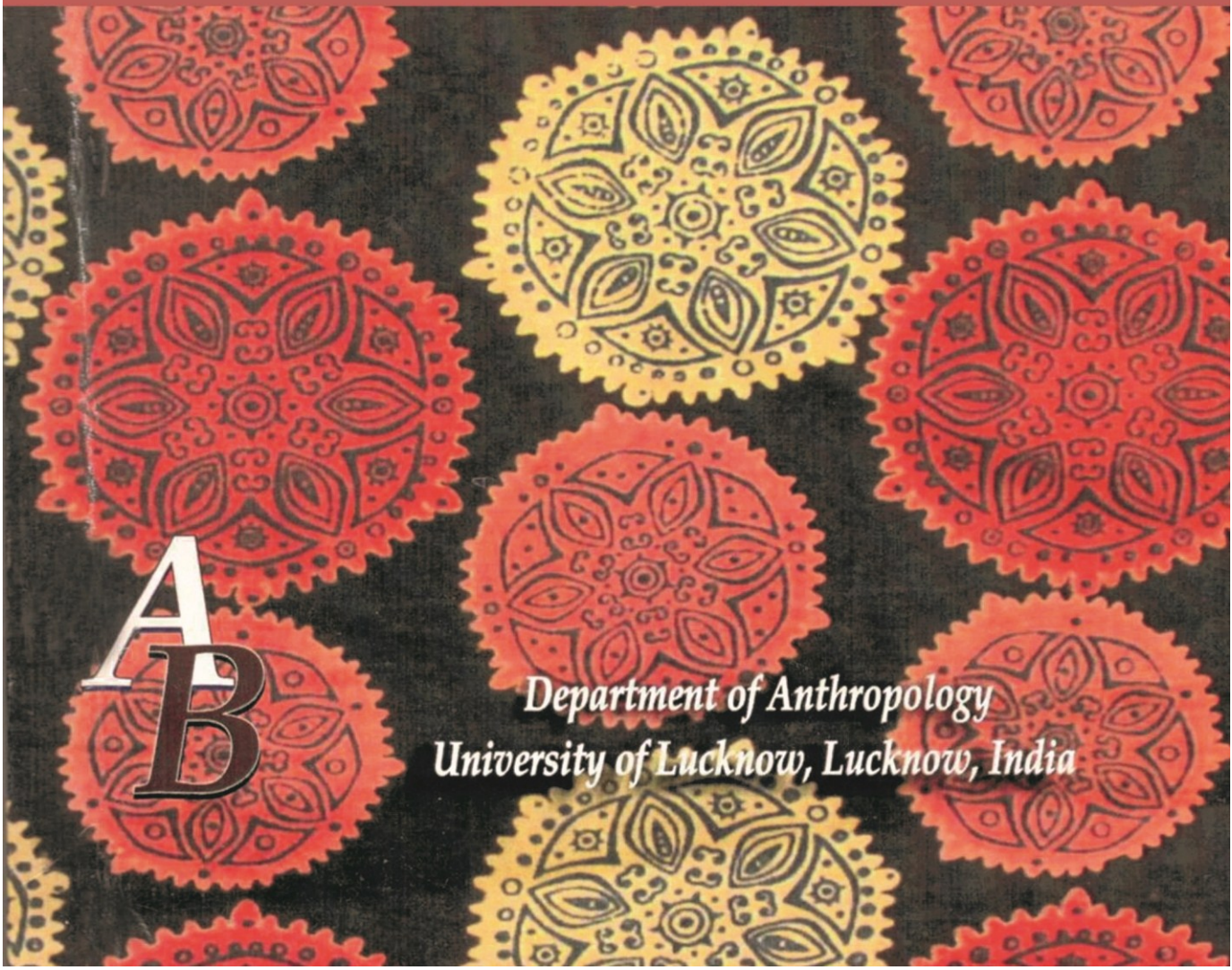
Volume 15, Issue 1
July 2020

ISSN No.:2348-4667

Anthropological Bulletin

a peer reviewed international journal



ISSN: 2348-4667
Anthropological Bulletin
15(1), 64-69, 2020

Blockchain Technology and Crypto Currencies: Regulatory and Technical Issues

Mohd Imran[♣]

ABSTRACT

The central question to be investigated in this paper is whether new technologies such as blockchain that enter various spheres of public life are safe for users and how they could impact national legislations. Cryptocurrencies, which are based on blockchain technology, can be used as a means of payment, investment or capital accumulation. Therefore, blockchain becomes more and more popular. The introductory part of the paper contains a general historical outline and basic principles related to blockchain technology. Real and potential threats posed by this technology are also to be discussed in the paper as well as the question whether governments or, more broadly, the international community, offer sufficient level of protection against risks related to the use of new technologies such as blockchain and cryptocurrencies.

Keywords: Blockchain Technology, Cryptocurrency, Distributed Ledger Technology (DLT), Peer-to-Peer (P2P) Network, Decentralization., Blockchain Security, Regulatory Challenges

Introduction:

A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. To use a basic analogy, it is easier to steal a cookie from a cookie jar, kept in a secluded place, than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people.[i]

Bitcoin, the decentralized peer-to-peer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world[ii]. However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully

♣ Assistant Professor in IPR, Z.H. College of Engineering & Technology, Aligarh Muslim University, India

applied to both financial and non-financial world applications. Last year, Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the blockchain distributed consensus model as the most important invention since the Internet itself. Johann Palychata from BNP Paribas wrote in the Quintessence magazine that bitcoin's blockchain, the software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond[iii].

Historical Evolution:

The history of blockchain and cryptocurrencies starts on the internet in November 2008 when an individual (or group) writing under the name of Satoshi Nakamoto published a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System"[iv]. This paper described a peer-to-peer version of the electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution. Bitcoin was the first realization of this concept. It defined and described a new digital currency, based on the idea of cryptographic linking of data blocks i.e. blockchain. The idea was entirely based on the computer technology and did not need any intermediaries such as human beings or institutions. The new currency was given a name Bitcoin and in no time at all it grew in popularity and value. In the initial phase blockchain was closely associated with Bitcoin only. However, with time blockchain technology has become an independent solution that can be used for many other purposes, for example, to improve payment processes, for data storage and transactions[v].

Basic Principles of Blockchain Technology:

The most distinctive feature of blockchain technology is that it does not require the involvement of a third party (e.g., banks, public registries, etc.) for transfers of value, whilst providing the parties involved in the transaction with absolute confidence in the validity and security of the transaction. Such transacting parties can be assured of the validity and security of the transaction due to the cryptographic proof of authenticity provided by the blockchain technology. Whereas a transaction needs to be verified by the central server in traditional databases, with blockchain technology, every node in the system has the ability to cryptographically check and verify any transaction. Instead of having to trust the central server (and the central authority maintaining such a server), peers using blockchain technology are able to create and maintain trust by relying on cryptographical proof in a consensus method. This feature obviates the need for the involvement of a third party in such transactions and is the main differentiator from (and improvement on) systems using traditional databases or ledgers. In other words, blockchain has no central server. The system consists of a large number of "nodes" that are continuously checking and confirming the validity of all transactions, instead of just a few such nodes. This distinguishing facet of blockchain technology eliminates (or, at least, seriously mitigates) the security vulnerabilities associated with traditional central databases[vi].

Another important blockchain classification concerns the distinction between public and "permissioned" ones. A blockchain can be configured in such a way that it allows everyone to become a node and verify/reject transactions. Such blockchains are available to anyone with an internet connection. Once the application running on the blockchain is downloaded to a smartphone or computer, participation in the verification system occurs automatically and takes place in the background. Therefore, while the system is highly secure, every piece of data produced from the moment that the blockchain begins operating is shared amongst every node (although they are cryptographically anonymized). On the other hand, blockchains can also be configured in a permission-based manner. These blockchains operate based on private networks. To become a node in such a blockchain, one needs to obtain permission from the system. For instance, in the (public) Bitcoin blockchain, one only needs to download a "Bit- coin wallet" from the internet to start participating in the verification

system. However, for a permissioned blockchain, one needs to get permission from the administrator of the blockchain to create a blockchain wallet and possibly obtain another authorization to become a node in the verification system. Blockchains also might be configured in a combined way in terms of public and private by granting such authorizations to specified accounts while anyone can have an account and perform certain actions[vii].

Technical Aspect:

The basic condition for the operation of a blockchain is the acquisition of the Peer-to-Peer (P2P) network concept. P2P refers to computer networks that use decentralized and distributed architecture. This means that all computers and devices have a specific share in the network. All connections of the network (hosts) have equal rights with no centralized administrator. These hosts communicate all the resources and data available in the P2P network to each other, without having to use a centralized server. The main purpose of this network is to allow direct networking of network devices. Peer-to-Peer networks are commonly used to transfer files over the internet, allowing hosts to send and receive them simultaneously. The main feature and advantage of this technology is decentralization and participation in the process of transaction authentication by all users who democratically approve a given operation without any control or supervision from above. An important thing about this technology is that instead of one central host, several decentralized hosts are used at the same time to download data fragmentarily. Another thing worth mentioning is the so-called distributed ledger technology (DLT)[viii]. It is a record of information or a database distributed in the network. Access to DLT can be open or closed. Blockchain is one of the varieties of the distributed registry and in itself is a collection of information from computers that are connected by a Peer-to-Peer network. Blockchain technology (as opposed to Bitcoin) can store data of various contents (not only related to exchange and payments). What is important, data transmission in the network takes place in an encrypted form, which allows to secure the transaction. During a new transaction, the host extends the set for new information, and other verifying hosts must confirm its correctness in accordance with the accepted rules, so that it can be added to the block. Each block contains a unique identifier of the so-called (hash) of the previous block that links the blocks into a sequence.

The system of distributed registers described above offers many benefits. In contrast to centralized systems, the network functionality is maintained even in case of failure of individual joints. This increases the trust and security of transactions, because people do not have to assess the credibility of the intermediary or other network participants. It is enough for users to build trust in the system as a whole. The absence of intermediaries also promotes data security. The current practice of external entities collecting personal data implies a risk of breach of security, while in case of blockchain, the data collected by third parties may become obsolete, which ultimately increases the user's safety.

Threats and Security Issues:

The whole point of using a blockchain is to let people—in particular, people who don't trust one another—share valuable data in a secure, tamperproof way. That's because blockchains store data using sophisticated math and innovative software rules that are extremely difficult for attackers to manipulate. But the security of even the best-designed blockchain systems can fail in places where the fancy math and software rules come into contact with humans, who are skilled cheaters, in the real world, where things can get messy.

To understand why, start with what makes blockchains "secure" in principle. Bitcoin is a good example. In Bitcoin's blockchain, the shared data is the history of every Bitcoin transaction ever made: an accounting ledger. The ledger is stored in multiple copies on a network of computers, called "nodes." Each time someone submits a transaction to the ledger, the nodes check to make sure the transaction is valid—that whoever spent a bitcoin

had a bitcoin to spend. A subset of them competes to package valid transactions into "blocks" and add them to a chain of previous ones. The owners of these nodes are called miners. Miners who successfully add new blocks to the chain earn bitcoins as a reward.

What makes this system theoretically tamperproof is two things: a cryptographic fingerprint unique to each block, and a "consensus protocol," the process by which the nodes in the network agree on a shared history[ix].

The fingerprint, called a hash, takes a lot of computing time and energy to generate initially. It thus serves as proof that the miner who added the block to the blockchain did the computational work to earn a bitcoin reward (for this reason, Bitcoin is said to use a "proof-of-work" protocol). It also serves as a kind of seal, since altering the block would require generating a new hash. Verifying whether or not the hash matches its block, however, is easy, and once the nodes have done so they update their respective copies of the blockchain with the new block. This is the consensus protocol.

The final security element is that the hashes also serve as the links in the blockchain: each block includes the previous block's unique hash. So if you want to change an entry in the ledger retroactively, you have to calculate a new hash not only for the block it's in but also for every subsequent block. And you have to do this faster than the other nodes can add new blocks to the chain. So unless you have computers that are more powerful than the rest of the nodes combined (and even then, success isn't guaranteed), any blocks you add will conflict with existing ones, and the other nodes will automatically reject your alterations. This is what makes the blockchain tamperproof, or "immutable."

Regulatory issues:

Blockchain technology will face various challenges from at least four different aspects, namely: (i) technical, (ii) marketing/business, (iii) behavioural/educational, and (iv) legal/regulatory[x]. For the purposes of this paper, our main focus will be the potential legal and regulatory challenges to this emerging technology. One of the most significant challenges currently facing blockchain technology, which should be of crucial interest to any legal practitioner, arises from the use of blockchain as a transaction platform. This is because a blockchain network can validate a variety of value-related transactions relating to digital money or assets that have been digitized[xi].Value- related transactions encompass, besides monetary transactions, transactions relating to land, debt, or intellectual property. The fundamental problem currently facing blockchain concerns the speed with which these transactions can be processed through blockchain technology. Compared to traditional transaction platforms, such as VISA or PayPal, blockchain is significantly slower at this time. For example, if we examine the transaction processing capacity of the Bitcoin blockchain (which is the most widely adopted and heavily used blockchain), we observe that it can handle 2–5 transactions-per-second ("TPS"), whereas VISA can handle 56,000 TPS and PayPal can process 155 TPS. However, it is worth noting that "some other blockchains are faster than Bit- coin's. For example, Ethereum started with 10 TPS in 2015, edged towards 50–100 TPS in 2017, and targeting 50,000–100,000 TPS by 2019.

As to the legal challenges ahead, the primary obstacle worth discussing is clearly the lack of adequate regulations and the absence of a proper legal framework with regard to blockchains. In recent years, blockchain technology has emerged and developed much more quickly than anticipated and we observe numerous applications of this technology that are creating new grey areas in light of the existing and inadequate regulations. For instance, the use of various cryptocurrencies to carry out illegal transactions on the Darknet markets was the first regulatory challenge posed by blockchain technology. Such unlawful behaviour forced regulators swiftly to implement certain regulations in this field in order to combat money laundering[xii]. Furthermore, a second wave of regulatory uncertainty arose from Initial

Coin Offerings ("ICO"), which were adopted as a crowdfunding method using cryptocurrencies. While countless scams have unfortunately occurred in recent years regarding ICOs[xiii],the declarations from regulatory authorities (such as the Securities and Exchange Commission in the United States (SEC))[xiv]have also played a significant role in a market that has reached a market cap of around 58 billion USD. The involvement of regulatory authorities (especially securities authorities) aimed to clarify the situation surrounding ICOs and try to protect the investors from the scams, but yet in a timid way. Since the underlying technology is still young and rapidly evolving (and has not been completely understood by the regulatory bodies), it is difficult and risky to impose regulations without fully understanding the consequences of such regulation. However, as could be expected, the lack of comprehensive regulation creates uncertainty regarding the future of blockchain technology and slows down the rate of adoption of this promising technology by global companies in their daily operations.

Another important legal challenge is the lack of planning concerning the legal requirements in the early blockchain platforms. Most of these platforms were focused on transactions and not nearly as much on their reporting obligations. This lack of foresight has now forced these platforms conducting value transfers to devise new solutions with respect to the reporting problem. Even though the lack of smooth and efficient reporting processes now may seem likely to cause problems in terms of taxation, it should be remembered that blockchain technology also holds great promise in terms of alleviating today's reporting problems and significantly improving current reporting processes, since such transactions are traceable and irreversible[xv].

Conclusion:

In the light of our foregoing discussion on the technical, legal issues surrounding this technology it is imperative that the advantages and benefits of blockchain are remarkable, though there are still various challenges ahead from a technical and legal aspect. There is an urgent requirement of awareness and understanding about this technology among the lawmakers, government regulatory bodies and the society at large as it appears that people are hesitant on relying this new technology. This is the first barrier to be crossed. It is undeniable that the technology gained much attention in recent years but the characteristic of the attention is also important considering the number of the news popping out day by day about an ICO scam or usage of cryptocurrencies in the black markets. Once the barrier of social acceptance is broken, it is no surprise that blockchain will gain attention not only as a source of quick return investment but also as a technology that may cause considerable benefit to many areas. At that point, regulations could be aiming at the best use of this technology rather than attempting to restrict or prohibit the technology or the products and services associated with the technology.

Suggestion:

The first action that could be taken by regulators is to grant legal status to blockchains and to define the standards that blockchains will have to meet in order to receive such legal status. The standardization work has already been commenced by the International Organization for Standardization (ISO). For example, ISO is currently working on its ICO/TC 307 standards for blockchain and distributed ledger technologies[xvi]. Once the framework and rules of standardization are established and are available for use by the developers, the ball will then be in the regulators' court to bestow blockchain with certain legal status. The standardization is also needed for the users (i.e. public, in most of the cases) since there are already variety of blockchains to be used in the market. The user must have the reliable information to choose the blockchain with the standards defined by the authorities. In a way, authorities should help the users with their choice of applications and

blockchain usage by creating widely accepted standards. That would lead users to proper application and blockchain for their use and motivate the developers to the end that they develop projects meeting the requirements of the standards.

It is also essential to consider the position of the blockchains with respect to existing regulations. There are numerous laws regulating the fields of communication and the internet. Sadly, most of these laws have been drafted and passed without considering the next layer of the internet or to future technologies. Therefore, some areas that are affected by blockchain technology are blank spots, legislatively speaking, and require effective regulation. However, the bigger problem may arise with respect to the areas that are already regulated. Such regulations may slow down the adoption or development of blockchain technology; therefore, the first step that must be taken is accurately mapping blockchain's potential effects and determining whether they fall under existing laws and, if so, how they are covered by such laws.

References

Online Resources:

http://www.risktech-forum.com/opinion/a-risk-based-view-of-why-banks-are-experimenting-with-bitcoin-and-the-block.
https://bitcoin.org/bitcoin.pdf
https: //www.ideals.illinois.edu/bitstream/handle/2142/97207/ hildenbrandt- saxena- zhu- rodrigues-guth- daian- rosu- 2017- tr _
http://elaineshi.com/docs/bitcoin.pdf
https://abovethelaw.com/2014/10/movie-night-with-justice-breyer/
https://cointelegraph.com/news/dont-believe-the-hype-the-five-largest-ico-exit-scams-expert-take
https://www.iso.org/committee/6266604.html

---

i Micha Crosby et al, Blochchain Technology: Beyond Bitcoin,02, Applied Innovation Review.8 (2016)
ii Id at 8.
iii Joram Borenstein, Spotlight on Risk Technology, A Risk Based View of Why Banks are Experimenting with Bitcoin and the Blockchain (Sept. 30, 2019, 4.31PM),
iv Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (Oct. 02.2019, 8.45PM)
v How Does Blockchain Works, Blockchain Technology and its potential in Taxes, (Sept. 28,2019, 9.30 AM)
vi William Mougayar, The Business Blockchain: Promise, practice and Application of the Next Internet Technology, P.4 (1st Edn. 2016)
vii Hidenbrandt et al, A complete semantics of the Ethereum Virtual Machine (sept. 20,2019, 4.10 PM)
viii Tomasz Slapczynski, Blockchain technology and Cryptocurrencies- legal and tax aspects, 23 Scientific journal of Bielsko-Biala School of Finance and Law 1-2 (2019).
ix Barber et al., Theft or Loss of Bitcoins, Bitter to Better — How to Make Bitcoin a Better Currency (Sept. 22,2019 2.30 PM)
x Supra note 6 at 66.
xi Ibi.
xii Nejc Novak, EU Introduces Crypto Anti- Money Laundering Regulation (Sept. 22, 2019 11.45 AM)
xiii Brian Kean, Don't Believe the Hype. Five Largest ICO "Exit Scams": Expert Take (Oct. 7. 2019, 10.45 AM)
xiv US Securities and Exchange Commission, SEC Issues Investigative Report Concluding DAO tokens, a Digital Asset, Were Securities
xv Gonec et al., Intellectual Property Law and Practice in the Blockchain Realm, 34, Computer Law and Security Review, 850 (2018)
xvi ISO/TC, Blockchain and Distributed Ledger Technologies

****