THINK INDIA (Quarterly Journal)

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

Critical Review of Blockchain Technology: Opportunities and Challenges

Atul Gupta
Assistant Professor in Commerce, Hindu College, University of Delhi, India.

Kartik Naahal, Ajay Deswal, Sidharth Yadav
(Students of Hindu College working under Innovative technologies project)

Abstract: Blockchain technology, an alternative to traditional ledger system based on the concept of decentralisation, anonymity and consensus approach possesses a great potential for the future internet system, it provides a solution to the numerous problems pertaining to data and information such as storage, transparency,privacy, data integrity and intermediation.The current study uses explorative approach to understand, discuss and bring out the issue relevant to the title. Secondary data and publications have been used to do this study. Entire paper is based on research papers, books, reports and government publications. Our study is mainly understanding the blockchain technology covering the elements, features and mechanism followed by the applications (financial and non financial) and the future purview tackling all the challenges and opportunities globally.

Key Words: Blockchain; cryptocurrencies; bitcoin; data privacy.

1. Introduction:

Modernisation and advancement proliferating in machine learning, computer technology and the Internet have completely changed the way we live. In the words of Brad Shapcott- "The Internet isn't free. It just has an economy that makes more sense to capitalism." It has grown so big and powerful that for some people it has become a complete substitute for life. Internet was a big revolution globally but now we are on the brink of another revolution, the next big thing after Internet- Blockchain Technology.

This revolution started with a new fringe economy on the Internet, an alternative currency called Bitcoin that was issued and backed not by a central authority, but by automated consensus among trustless networked users. Under the pseudonym, a person or a group named Satoshi Nakamoto in 2008 published the bitcoin white paper which explicated it as 'a peer to peer' version of electronic cash that would make online payments to be sent directly between parties without any intermediary involved, thus reducing the cost and improving the efficiency of transaction. Blockchain' is the fundamental technology for the Bitcoin. Though the most popular example that is intrinsically tied to Blockchain Technology is Bitcoin but nowadays it has diversified much more than bitcoin only.

In simple terms, blockchain means the public ledger of transactions stored in a chain of blocks that have been incurred till now. The blocks in the chain constantly grows as miners (who secures the network and processes every transaction) add new blocks to it for recording the most recent transaction. It stores the complete information about addresses and balances originating from genesis block (the very first block in the transaction) to the most recent block executed. Participants in the system substantiate each transaction by consensus of a majority of the nodes (every computer connected to the network). While validating a distributed consensus

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

where each and every online transaction gets verified at any time in the future, it serves as a huge potential to revolutionize the digital world and all of this is done without compromising the privacy of the digital assets and parties involved. Along with the distributed consensus, features of Blockchain such as disintermediation and decentralisation allows all transactions of any type between all parties on a global basis. When a data is stored through a transaction on the blockchain, eventually it becomes immutable in practice.

Despite the fact that the blockchain technology has great potential for the construction of the future internet systems, it is facing some technical challenges as well. Scalability and data privacy are the main animadversions of blockchain. Bitcoinblocksize is limited to 1MB and is restricted to a rate of 7 transactions per second which is susceptible to deal with high-frequency trading. Also, blocksize and propagation speed are inversely related, thus large blocks mean larger storage space but slower propagation in the network and vice versa. Thus, tradeoff between block size and security has become a huge challenge. The privacy setting is also limited since there are no selective users, and every participant can join the network and can access the distributed ledgers. The other challenge to blockchain technology is 'Quantum Computer', with its sheer brute force approach a quantum computer can easily crack the cryptographic keys within reasonable time and bring the whole blockchain system to its knees.

But, with revolutionary potential equal to that of Internet, Blockchain technology could be established and embraced much more faster, provided the network upshots of contemporary access of global internet and cellular connectivity.

2. Literature Review:

[1](Primavera de Filippi, 2016) Author talks about the use of blockchain and how it can be used specifically in crowdfunding (the practice of funding a project or venture by raising small amounts of money from a large number of people, typically via the Internet e.g. Kickstarter, Indiegogo, etc.) . Since there are no intermediaries and comparatively low transactional cost, people can engage more directly with their favourite artists and pay them directly without having to rely on intermediaries. This literature also talks about an innovation about how blockchain can be used to create a new type of securities which represents shares of the project for which the funds are sought, instead of being rewarded with predefined perk. Therefore benefit from any additional revenue that might derive from the subsequent appreciation in value of these shares.

[2] (Larissa Lee,2016) Literature talks about blockchain in great details from what blockchain actually is to how a transaction actually happens and whether blockchain be able to replace traditional stock market. Literature draws an in-depth comparison between traditional stock market with one that is influenced by blockchain. According to author, Blockchain is just an alternative to traditional stock market, not a replacement. It's for those who are not satisfied with the current regime and it's likely that there will be a need for both the systems.

[3] (ZibinZheng, ShaoanXie, Hongning Dai, Xiangping Chen and Huaimin Wang, 2017) Authors have presented a comprehensive overview on Blockchain Technology, starting with the applications of blockchain which arrays an advent of new revolution and potential for transforming traditional industry with its key characteristics. They have also talked about the

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

taxonomy of blockchain systems and different consensus algorithms followed by the technical challenges and existing approaches for solving these problems. Smart contracts, Big data analytics, blockchain testing and halting the tendency to centralization are some of the possible future directions mentioned broadly in the literature.

[4] (Michael Nofer, Peter Gomber, Oliver Hinz and Dirk Schiereck, 2017) Financial Industry is seen as the predominant application of the blockchain driven by substantial process inefficiencies and a massive cost base issue specifically in this industry. Literature represents blockchain as a shift from trusting people to trusting math. Authors have talked about the functionalities and implications of blockchain, talked about the (Lewenberg, 2015) concept of "Inclusive Block Chain Protocols" and how (Fairfield, 2014) smart contracts can also be used to control the ownership of properties. It has widely mentioned the applications of Blockchain in both Financial (Cryptocurrencies, insurance, trading and settlement) and non-financial (notary public, music industry, internet applications, decentralized proof of existence of documents, internet of things and anti-counterfeit solutions) world.

[5] (Michael Crosby, Nachiappan, PradanPattanayak, SanjeevVerma, Vignesh Kalyanaraman,2016) The implementation of Blockchain Technology is pretty much successful in both financial and non-financial world. Marc Andreessen listed the blockchain distributed consensus model as the most important invention since the Internet itself. Palychata from BNP had written in Quintessence magazine that blockchain technology should be considered as an invention similar to steam engines that has the potential to transform the world of finance and beyond.

[6] (Kelly, Jemima; 2016) Big Tech Companies like Samsung, Amazon, IBM, Ebay, Citi and Verizon Wireless are all looking alternative and novel uses of this technology. In September 2015, in order to create a framework for using Blockchain Technology in the financial market, 'Barclays and Sachs' and some 8 other biggest banks in the world have come together and recently joined forces with the financial technology firm named 'R3', a New York based firm.

[7] (YinkiaChiam, Sin Kuang Lo, Qinghua Lu, 2017) Blockchain may be an appurtenant choice for some use cases while traditional technologies will be more appurtenant for other cases. In this paper, based on the characteristics of the use cases, the authors proposed an evaluation framework that comprises a list of criteria and a typical process for practitioners to assess the suitability of applying blockchain using these criteria. Then they rolled out several existing industrial trails to evaluate the practicability of their framework. A major difficulty for practitioners to decide whether or not to use blockchain is limited product data or reliable technology evaluation availability to assess the suitability of blockchain.

[8] (WitoldNowiński, MiklósKozma, 2017) Blockchain technology is gaining momentum with more and more diverse applications, as well as increasing numbers of actors involved in its applications. Literature talks about possible applications of blockchain technology to businesses, and in particular how it can disrupt business models. Authors proposed that there are three crucial ways in which blockchain technology can affect and disrupt business models: by authenticating traded goods, via disintermediation and lowering transaction costs. It is important to note that blockchain is going to affect not only the companies which comply to this technology but also those companies which have to restructure their business as blockchain undermines their offering.

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

[9] (RifaHanifatunnisa and Budi Rahardjo, 2017) Since Blockchain embraces a decentralized system, literature has comprehended it as a solution to the data manipulation, security, transparency and centralized system of general elections. This research proposed a database recording system and design on e-voting using blockchain technology and bitcoin system. Method mentioned in the literature aims to maintain data integrity, which is protected from manipulations that should not happen in the election process. In brief five steps have been proposed in the entire methodology starting with the Verification, getting a turn, update database, creating new block and concluding with broadcast. Hash values linked to each other blocks along with digital signatures make the E-voting more reliable.

[10] (Jong-Hyouk Lee, 2017) Literature has considered Blockchain as a functional technology for improving existing technologies and creating new applications previously never practical. Author has introduced Blockchain as a new ID as a service for digital identity management. Creation of BIDaasblockchain, where the BIDaas provider and its partners have permission to access, provides required information for IDaaS. An example for mobile users of a mobile telecommunication company is also mentioned in the literature providing practicality of the methodology. Procedure of BIDaas is started with Virtual ID creation, BIDaasblockchain registration, mutual authentication and extra information request. Implementation of the same as cloud platform, developing a secure TEE operation for the mobile user case which provides the most secure area that guarantees code and data loaded inside to be protected in terms of confidentiality and integrity are schemes to detect or prevent misuse of the provided user information at the partner.

[11] (NASDAQ, Chain; 2016) The American stock Exchange NASDAQ launched its private equity exchange in 2014.NASDAQ joined hands with a San Francisco based startup named 'chain.com' to avoid inefficient and slow trading of stocks and to implement private equity exchange on top of Blockchain as it previously involved multiple 3rd parties in the exchange process. Blockchain based smart contracts are being implemented by chain.com for smooth, transparent and efficient exchange functionality.

[12] (Infante, Andre; 2016) The very concept of Blockchain technology lies with the fact that miners continuously with their coding powers create blocks to be added to the blockchain which makes it near impossible for a single party to game the system and make changes from the very beginning of the chain. But with the modern scientific development and emergence of 'Quantum Computers', the cryptographic keys may be cracked easily within a short period of time through sheer brute approach. With the development of this technology, the entire Blockchain technology system will be brought to its knee.

[13] (Jesse Yli-Huumo, DeokyoonKo, Sujin Choi, Sooyong Park, Kari Smolander, 2016) Blockchain is a decentralized transaction and firstly data management technology developed for Bitcoincryptocurrency. The reason for the increasing interest in Blockchain is its central attributes that provide security, anonymity and data integrity without any third party organization in control of the transactions. In this research, the authors have conducted a systematic mapping study with the goal of collecting all relevant research on Blockchain technology.

[14] (Alex Castro, 2018) Even though blockchain technology was first introduced in the year 2008, when Satoshi Nakamoto - a pseudonym- published a paper outlining the idea revolving around bitcoin, there still does not exist a universal definition of a blockchain. In this article,

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

the author analyzes definitions given by many well reputed sources like Google, IBM, Investopediaetc just to find out that each definition has one flaw or the other. The author also pointed out the rush some state are into pass some sort of legislation to demonstrate how crypto-friendly or tech-savvy they are. He also quotes Victoria Lemieux, an associate professor of archival science and head of the blockchain research cluster at the University of British Columbia and unfortunately she estimated the terminology standard will take approximately 18 months to be finalized.

[15] (Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system) Comprised by the founder of bitcoin itself, literature comprises of fundamentals of bitcoin, timestamp server, proof of work (consensus algorithm), network, incentives, privacy and calculations. It proposed a system for electronic transactions without relying on trust starting with the framework of coins made from digital signatures which provides strong control of ownership. To prevent double spending, they have proposed proof of work (a peer to peer network) to record a public history of transactions. In the system proposed, reversible transactions are possible which spreads the trust. Since methodology doesn't require any mediation, transactions cost reduces further improving the efficiency of transactions as well.

[16] (AsaphAzaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman, 2016) Literature has proposed a new system for medical data access and permission management using blockchain technology that is MedRec. Using Medrec authors have proposed a solution to time delay, bulky record maintenance, charging exorbitant prices for data exchange interfaces, interoperability between different provider and hospital systems that pose additional barriers to effective data sharing. By prioritizing the patient agency MedRec serves as a benefit for patients from a holistic, transparent picture of their medical history. MedRec is build on distributed ledger protocol originally associated with Bitcoin which uses public key cryptography to create an append-only, immutable, timestamped chain of content. MedRec gives patients a log of their medical history, which is not only comprehensive, but also accessible and credible.

[17] (S.Meiklejohn, M.Pomarole, G.Jordan, K.Levchenko, D.McCoy,G.M. Voelker, and S. Savage, D. Ron and A. Shamir; 2013) The transactions in a Blockchain technology are made with the pseudonymous identity of the parties related to transactions. But despite the fact that parties can create pseudonymous public keys to increase their anonymity, the record of all transactions of every individual public keys are publicly visible. Being the fact that the present form of these transactions lacks transactional privacy, recent works have demonstrated the deanonymization attacks through analyzing the graph of transactions that are made by every pseudonymous identity.

[18] (HBR- The Truth About Blockchain; 2017) There's hype about the Blockchain technology that it's going to transform and revolutionize business. But this technology is like TCP/IP (technology on which the internet was built) i.e. blockchain is foundational technology that will require broad coordination and like TCP/IP, its adoption will follow a fairly predictable path and this journey will take years. Adopting a foundational technology typically happens in 4 phases. Every phase defines the novelty of application and the complexity of efforts required to make them practically use. Low novelty applications and complexity tend to gain acceptance first. While, applications high in novelty and complexity take decades to evolve while having the potential to transform the economy.

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

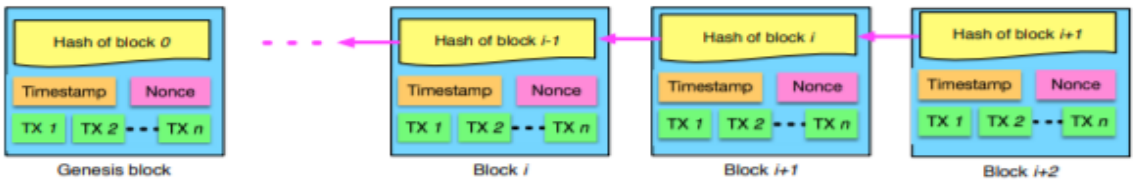
[19] (ZibinZheng, ShaoanXie, Hong-Ning Dai, Xiangping Chen and Huaimin Wang, 2018) Literature talks about the numerous benefits of blockchain such as decentralisation, persistency, anonymity and auditability. Blockchain technology has great potential for the construction of the future internet systems, though it is facing a number of technical challenges which are scalability, propagation speed, privacy leakage and selfish mining. Authors have also talked about the taxonomy of blockchain systems which includes consensus algorithms, read permission, immutability, efficiency and centralisation. Finance, Internet of things (IOT, public and social services, reputation system, security and privacy are some of the applications of blockchain explained in literature. Blockchain testing, halting the tendency to centralisation, big data analytics, smart contract and artificial intelligence are the possible future directions in the relevant field.

[20] (Tiffany Wan, Max Hoblitzell; 2014) With the evolution of Bitcoin, new cases will continue to emerge, opening up a wide range of new opportunities, along with emerging challenges for governments and businesses across various industries. Businesses will change the way they operate as Bitcoin has the potential to change the way government manages the market & implement laws. Bitcoin Technology i.e. Blockchain could soon disrupt other systems that rely on intermediaries including transfer of property, execution of contracts and also identity management.

3. Blockchain Architecture:

Series of blocks interconnected to each other in a prescribed format forms a blockchain, which hold details of all the transactions happened like a conventional public ledger does. Each block is attached to a previous block through a unique reference number that is a hash value of the previous block called as parent block. Only one block in the chain does not have any parent block that is the first block known as genesis block.

3.1 Block Each block can be thought of as a page in the ledger where all the data pertaining to the transactions are stored. The individual blocks are composed of several components. It consists of the block header and block body as shown in figure 1.



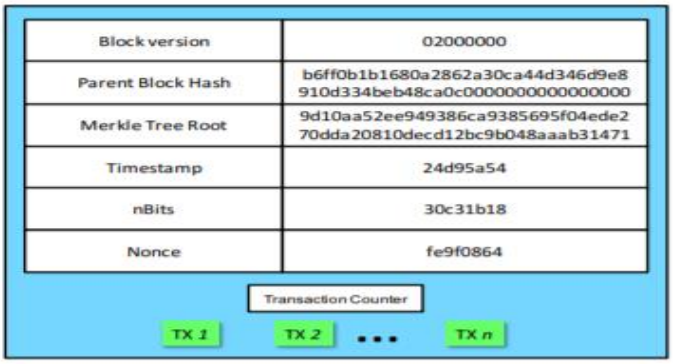
(ZibinZheng, ShaoanXie, Hong-Ning Dai, Xiangping Chen and Huaimin Wang, 2017) Figure 1

The head of the block is bifurcated into six components:

1. The version number of the software: In this a miner with a particular version number signals which set of block validation rules to follow.
2. The hash of the previous block: Parent block hash is a 256-bit hash value that is connected to the previous block. Without this component, there would be no connection or chronology between the blocks.

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

3. The root hash of the Merkle tree: All the transactions contained in a block can be aggregated in the hash value of all the transactions in a block. This is the Merkle tree root hash.
4. Timestamp: It is the current timestamp in the block itself. The time is given in seconds since 1.1.1970.
5. nBits: It indicates how small the new hash must be to claim validity. In particular, it validates the current hashing target in a compact format.
6. Nonce: It is kind of hash value, a 4-byte field, which usually starts with 0 and increases for every hash calculation. It is the variable incremented by the proof of work.



(ZibinZheng, ShaoanXie, Hong-Ning Dai, Xiangping Chen and Huaimin Wang, 2017) Figure 2

The block body is composed of a transaction counter and transactions. The limit on transactions which a block can contain depends on the block size and size of transactions. For example, on the bitcoin network each block can be a maximum of 1 MB. In the ethereum network a new block is appended every 15 seconds, whilst on the bitcoin network it is every 10 minutes.

3.2 Characteristics of Blockchain:

1. **Distributed ledger:** Unlike centralized transaction systems, information in blockchain is spread across all the blocks, thus to add or edit any information, you must take the consensus of the majority of the nodes connected in the network. In particular, it is based on the concept "Trusting people to trusting math." Thus, it can easily mitigate the performance bottlenecks at the central server, development and the operational cost incurred in the process.
2. **Consensus based:** A transaction on blockchain can be executed only if the majority of the nodes unanimously approve it. It helps to keep fraudulent transactions out of the database. However, rules pertaining to consensus can be altered to suit various circumstances.
3. **Auditability:** All the information pertaining to a transaction and also links to the previous transactions are stored in a through accessing any node in the distributed network. It makes the data more transparent and traceable stored in the blockchain.
4. **Immutability:** Once nodes have agreed on a transaction and recorded, it can never be changed. You cannot edit the data in the existing block but only have to add a

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

new block about that asset to change its state. Thus, whatever happened throughout its life and true state to that particular asset is accessible and can be find out easily.

5. **Anonymity:** Each user operates with a generated address through which it can interact in the network. Further, a user could generate many addresses to avoid any identity exposure. Typically, only the digital addresses with corresponding units are available on the blockchain, keeping the identities of the user hidden. This amounts to a certain amount of privacy on the transactions included in the blockchain.

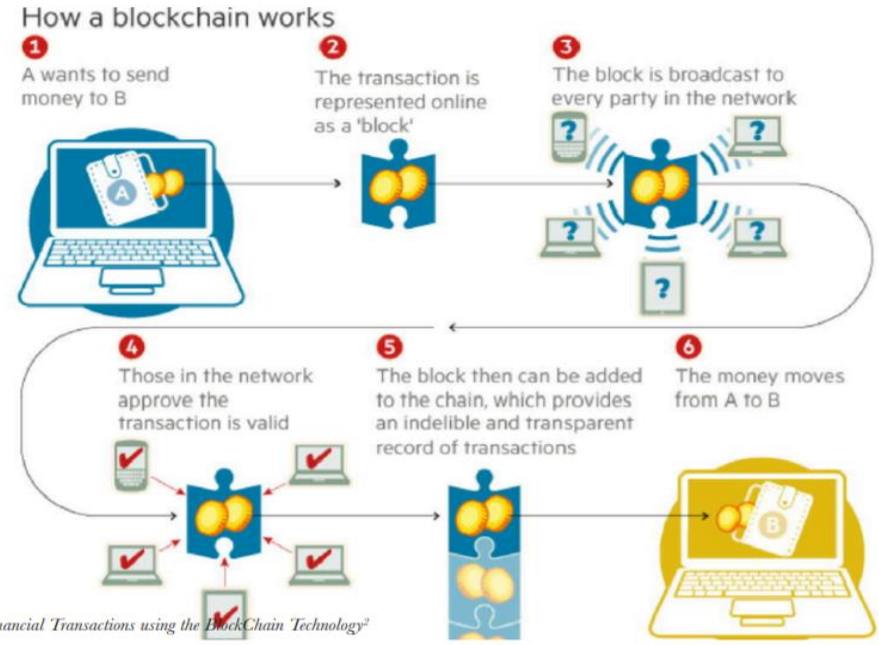


Figure 3: Financial Transactions using the BlockChain Technology

(Michael Crosby, Nachiappan, PradanPattanayak, SanjeevVerma and VigneshKalyanaraman, 2016) Figure 3

3.3 Advantages of Blockchain Technology:

1. Disintermediation: We are living in the age of disintermediation, all credit goes to blockchain. Blockchain is changing
the way business works. Disintermediation means reduction in the number of intermediaries between consumers and
producers.This means transactions between two parties is possible without the intermediation of a third party.

Blockchain aims introduce the following into a transaction economy:

- **Trade:** Blockchain allows trading property, currency, identity, reputation, or anything of value. This implies digitization of assets and establishment of a validity and reputation system in the surrounding economy.
- **Ownership:** Blockchain puts in place a system that is based on a trustless system and is still trusted by its users. That it does to support the ownership of digital goods and services.

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

- **Trust:** Blockchain creates a network that can store and ratify ledger entries, without being centralized. With blockchain, no single entity gets control of the system.

2. **Ecosystem simplification:** All transactions are added to a single public ledger. Hence reducing clutter and complexity of multiple ledgers.
3. **Empowered users:** Users are in control of all their information and transactions.
4. **Durability reliability and longevity:** Due to the decentralized networks, Blockchain does not have a centralized point of breaking down and is better able to hold out against malicious attacks.
5. **Transparency and immutability:** Any changes to public Blockchains are unconcealed creating transparency, and all transactions are immutable, meaning they cannot be altered or deleted.
6. **High quality data:** Blockchain data is consistent, complete, unerring, and broadly accessible.
7. **Lower transaction costs:** By eliminating third party intermediaries and overhead costs for exchanging assets, blockchain has the potential to greatly reduce transaction fees.
8. **Faster transactions:** Interbank transactions can take days before being cleared and finally settlement, especially outside of working hours. Blockchain transactions can reduce transaction times ranging from a few seconds to upto 10 minutes and are processed 24/7.
9. **Process integrity:** Users can trust that transactions will be executed exactly as per the protocol commands eliminating the need for an entrusted third party.

3.4 Challenges to Blockchain Technology

1. **Performance:** For users, blockchain performance is the speed at which they get the requested service. Any number of people can participate in the network, as it is public. There needs to be consensus on the network about the validity of the transaction in order for it to go through. While this system reduces the risk of malicious activity being carried out on the network, it can also increase the time it takes for transactions to settle. The Bitcoin can handle only three to seven transactions per second; the corresponding figure for Ethereum blockchain is as low as 15 transactions per second, Bitcoin and Ethereum being two of the biggest cryptocurrencies.
2. **Uncertain regulatory status:** Even as companies seek to integrate the distributed ledger technology into their business models, uncertainty about the regulatory landscape is seen as a major stumbling block.Regulatory issues is the prime challenge for permissionless public blockchains, since anyone can join and people are already moving significant amount. Though Regulators around the world have been working on how best to handle blockchain networks and the cryptocurrencies technology enables but it will still take some time until blockchain become widely acceptable.
3. **Large energy consumption:** According to new estimates published by researchers at the University of Cambridge, Bitcoin consumes more energy than the entire nation of Switzerland. Bitcoin Blockchain network's miners are attempting 450 thousand trillion solutions per second in efforts to validate transactions, using substantial amounts of computer power and electricity. Over the course of a year that's equal to around 64 TWh or terawatt hours of energy consumption. Bitcoin accounts for roughly 0.25 of the world's entire electricity consumption.
4. **Control, security and privacy:** Although solutions like private Blockchains (also known as permissioned blockchain) and stronger encryption exists, there are still many

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

cyber security concerns that need to be tackled before the general population can entrust their personal data to a Blockchain.

5. **Integration concerns:** Blockchain is a new technology that will require a significant change, if not a complete overhaul, to current system in order to adopt solutions offered by applications of blockchain. In order to make the switch, companies must strategize the transition.
6. **Untested at Full Scale:**Since the blockchains of today are as large as they have ever been, we are approaching unknown territory with every gigabyte of expansion. The limited experience in distributed ledger technology (in other words blockchain) means limited experience identifying and responding to problems.
7. **Decentralization is hard to guarantee:** In theory, the algorithm is still decentralized and anyone can try to compete, but in practice only those with the right hardware can justify the cost to win a seat at the virtual table. That leaves control in the hands of a few.

4. Mining

Everyone who has heard of Blockchain Technology and Bitcoin might also have heard of the term 'Mining'. Firstly, mining is not about creating new Bitcoins. So, what is mining? In simple terms, Mining is like a tool that secures the technology and allows blockchain to be a decentralized security by verifying its transaction information through blocks. Mining relies on some complex math done by miners (person involved in doing mining) to enable and maintain a system without central authority by securing the Blockchain system

Miners authorize every new transaction and register them on the global ledger known as Blockchain. Basically, miners compete among themselves to solve the complex math based on cryptographic hash algorithm. The solution to that algorithm is known as 'Proof-of-Work' which show the limit of resources and time spent by miners to come to a solution of the problem. On an average, every 10 minutes miners mine a block which is added to the Blockchain network. When a block is 'solved' using hash functions, the transaction contained in the blocks are considered as 'confirmed' and the digital currency (Bitcoin) concerned in the transactions can be spent. So, during a transaction in the Blockchain network, if you receive some digital currency on your wallet, it might take about 10 minutes for your transaction to be confirmed by miners.

Miners are incentivize for solving the complex mathematical problem i.e.'mining'. There are generally 2 ways to incentivize a miner and reward them for mining: new Bitcoins (in case of Bitcoin mining) or transaction fees.

4.1 Mining Process

The following steps explains how a transaction gets confirmed and is added to the blockchain network through mining (the process is explained with respect to 'Bitcoin Mining':

Step 1: A user on the blockchain network who in an attempt to send a specific quantity of crypto-coin (Bitcoin) to someone else signs off on a transaction from their wallet.

Step 2: The transaction from the user's wallet is then broadcasted on the respective blockchain network by the wallet application, waiting to be picked by a miner on the similar blockchain

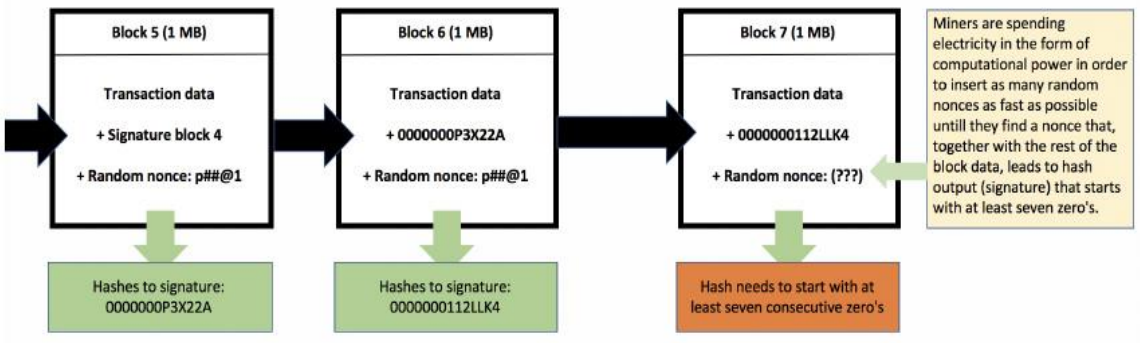
ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

network. However, if the transaction is not picked by the miner, it hovers in a 'unconfirmed transactions pool'. This pool consists of all the transactions that are not picked by miners on the network and are waiting to be processed. The 'pool' however is not a gigantic pool of all the unconfirmed transactions but its more like small sub-divided local pools.

Step 3: Miners (sometimes referred to as 'nodes') form 'block' by selecting the unconfirmed transactions form the pool. So, a 'Block' is a set of transactions (unconfirmed transactions at this point), in addition to some extra metadata. Each specific miner builds their own specific block of transactions. Also, a single transaction can be mined by multiple miners which is to be included in their block. But, each specific Blockchain has its own Block size (1MB in case of Bitcoin Blockchain), so every miner must check the blockchain history and then process the respective transaction if can be added to the block. Miners during mining generally prioritize and add that transaction to the block which offers high transaction fee set, as it incentivize a higher reward.

Step 4: Now a block of transactions is created after miner selects and adds the transaction to the block. For this block to be added to the blockchain (for all other miners and nodes to register the transactions), the block requires a signature (or Proof-of-Work) aka hash output. The signature which is unique to each block of transaction is created by solving a complex mathematical problem which is again unique to every block on the blockchain network, so every miner will work on a unique mathematical problem linked to every unique block.

Consider the data inside a block to be a hash input (string of data). When input is hashed, it gives hash output (a 32 digit string). The hash output string generated by the hash input string is always random for every different input string. However the same input string always generates the same output string. In case the input data string leads to signature which is not accepted by the blockchain network (eg. Rule of Bitcoin Blockchain is that the block can be added if the signature starts with certain quantity of zeros) then miners repeatedly change a part of data string inside the block called the **nonce**. Every time a nonce is changed, the input string is changed so ultimately the signature (output string) also changes as well. The process is indefinitely times performed by the miners until they find an output that meets the signature requirements (zeros in case of Bitcoin).



(Jimi S. May 3, 2018)

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

Note: the above process is apparently does not define a mathematical problem but rather a deterministic thing.

Step 5: After finding an eligible signature for the block, the miner broadcasts the block its signature to all other miners.

Step 6: Once the block is broadcasted, now other miners use the string of data of broadcasted block to verify the legitimacy of the signature by hashing it to see if the output hash indeed matches with the signature. If the output hash generated by miners to matches to the signature of the broadcast block, the other miners will confirm its validity and agree for the addition of the block to blockchain (the decision is taken by consensus). That's how the word 'Proof-of-Work' comes from because the signature is the proof of the work performed by computational powers.

The block is now added to the blockchain and is spread across all the nodes in the network. The other nodes in the system accepts the block and save it their respective transaction data.

Step 7: After successful addition of a block to the blockchain, every new block that is added on top of it counts as a 'confirmation' for that block. It's known as a 'confirmation' because for every new block to be added on top of previous block, the blockchain again reaches consensus to complete the transactional history including your transaction and your block. The more the confirmation a transaction on system has, the harder it maker for hackers to alter the details of blockchain.

After every new block is added to the blockchain system, miners are supposed to start over the mining process from step 3 by creating a new block of transactions. The reason why miners can't resume mining they were working on because of 2 reasons:

1. The data they on which they were previously working on might have been confirmed by the last block that was added to the chain and therefore these transactions may result in invalid results and thus making the block invalid.
2. Every block to be added needs signature of the previous block that has been added to the blockchain into their 'metadata'. So. If a miner continues to work on block containing data that has already been added to the blockchain, other miners will catch the hash output and will therefore reject the block.

5. Opportunities and Applications:

5.1 Stock Market: Securities and Exchange Board of India is persistently exploring how Blockchain can be used effectively in high frequency trading in stock markets. Markets can be more optimally utilised through automation and decentralization providing a huge potential for tracing securities lending, repo and margin financing and monitoring systemic risk. Tokyo stock exchange, New York stock exchange and Deutsche Borse are some of the examples who are already using blockchain as its core trading infrastructure or has shown their intent to evaluate its feasibility and advantages. Automation of post trade events, mechanism for fairness, transparency and risk containment, higher liquidity and lower transaction costs are some of the benefits that this technology will add to the stock markets.

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

Issues with traditional stock market and what a cryptocurrency market could do to solve them:

1. **Problems with stockbrokers:** Stockbrokers doesn't always have the best interest of the investors in mind. A Stockbroker's job is to make investor's money earn more money, while charging a fair fee for the service. Unfortunately, this is not the case every time. There are times when stockbrokers put their financial interests before the investor's. Although this is not the case most of the times. However, there's also a small, but ever-present contingent of fraudulent stock brokers that are drawn to the investment business because of the large dollars involved.
2. **High Frequency Trading:** High frequency trading involves buying and selling of securities in a fraction of a second. The main purpose of HFT is to make profit off of even the smallest changes in prices.The securities industry estimates that high-frequency trading accounts for more than half of all volume in the stock market. Critics of HFT argue that HFT firms are getting all the reward without taking any of the risk. Stephen Weiss of Short Hills Capital argued that HFT firms are not adding liquidity. They're sucking it out and returning it at a higher price after they've scalped you." Crypto Securities can solve some of the major issues with HFT's. Main element of HFT is its speed and it takes time to verify a crypto transaction, even the fastest crypto technologies take several seconds to get verified.
3. **Flash Crash:** A flash crash is when a market, whether stocks, bonds, or commodities, plummets within minutes and then rebounds.On May 6, 2010, in only twenty minutes, investors lost around $862 billion.However, within fifteen minutes, the market bounced back up toalmost exactly where it started that day. As securities trading has become a more heavily computerized industry driven by complicated algorithms across global networks, the propensity for glitches, errors and even flash crashes has risen. It takes an average of 10 minutes for a new block to be added to the blockchain, allowing enough time to verify each transaction before it is added to the transaction.

Advantages of crypto securities market

1. **Transparency:** All transactions on the Blockchain are public and can be traced from origin through to present day. Traders dissatisfied with the status quo and dark pool trading, who feel that the system is corrupt because of all the secret trading and problems on Wall Street are the ones who will appreciate the most.
2. **Improved Speed:** Even though high frequency traders can make transactions in microseconds, the actual delivery of shares can take upto 3 days. Transactions done on blockchain take about 10 minutes to get verified, hence making the ownership rights clear. Furthermore, blockchain is not restricted to a specific time frame, it runs 24 hours a day so traders will not have to worry about after hours trading.
3. **Cheaper Transaction cost:** Blockchain technology has the potential to reduce the transaction cost with cryptocurrency market. Since there are no intermediaries involved in blockchain, there will be no requirement of a stockbroker. The only cost involved will be the cost of transfer of funds from one account to another.

Even though crypto securities have a huge advantage over traditional stock market, a complete replacement is nearly impossible unless the government changes the laws regarding the same significantly. Furthermore, many players in the traditional stock market would have to be displaced overnight, including transfer agents, brokers, and the traditional stock exchanges. Even if the government does manage to change the laws, it is highly likely that there will always be a need for

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

both systems, just as with the rise of e-mail there is still a need for old post office to manage traditional letters.

5.2 Cryptocurrencies: Cryptocurrencies are the most vital and widely recognised application of the blockchain. Bitcoin, litecoin, ripple and monero are some of the examples in this category. In the coming times, in the financial industry, a large part of the current business might get replaced by the blockchain. Various government agencies, departments and courts have classified these digital assets differently and some of the countries even have come up with their own cryptocurrencies, for example The Bank of Thailand in August 2018, announced its plan to create their own cryptocurrency, the Central Bank Digital Currency (CBDC). We have already discussed a lot pertaining to bitcoin, Litecoin is an open source P2P digital currency that enables instant payments to anyone in the world and that can be efficiently mined with consumer grade hardware. Ripple is also a payment protocol founded by Chris Larsen, it is a real-time gross settlement system, currency exchange and remittance network which connects banks, payment providers, digital asset exchanges and corporates via RippleNet. Monero uses an obfuscated public ledger, meaning anybody can broadcast or send transactions, but no outside observer can tell the source, amount or destination.

5.3 Insurance: Any insurance policy exists as a contract between the insurance company (the insurer) and the policyholder (the party covered by the policy). Policyholders purchase a liability policy to protect their property, assets, and self. The hype cycle for the insurance sector depicts blockchain technology at the beginning of the curve connecting the technology trigger phase with the peak of inflated expectations, meaning that this technology has not been fully explored yet in the insurance sector. Services include compensation for any kind of injury or loss. The service providers are responsible to help insured find out if specific rules are met, the insurers exchange all of the information. So, if they can ensure that a particular event happened and the specific rules are met, then the customer will get the related money.

Advantages of Blockchain in Insurance Sector:

- The higher end of efficiency, making the process simple.
- Rapid turnaround time for an insurance claim.
- No risk of fraudulent activities.
- Premium policy reduction.
- A better experience.
- Automated paychecks.

Use cases of Blockchain

- **Auto Insurance Claims:** The connection between parties is imperative for auto insurance to avoid any fraudulent claims and to accelerate the process in general. With the help of smart contracts, specific parties can be notified so that necessary actions could be taken swiftly. With further advancements in technology, insurers may even be able to track every vehicle and assess the damage without any help.

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

- **Health Insurance:** Medical institutes are in dire need for a technology that can link all parts of medical institute, to help process insurance claims, along with tending to their data security issues. Blockchain offers all that and more.
- **Life Insurance:** Claiming a life insurance policy after a person dies is a complex process. Insurer needs to figure out if the death was legitimate or if any other fraudulent activity occurred or not along with many other things. Blockchain can eliminate the need for a middleman and help to process the grief without worrying about the insurance. Every facility from the hospital to the funeral organization will get connected in the network via blockchain.
- **Improving the Trust:** Insurance companies try their best not to process an insurance claim. This is why people get less interested in obtaining insurance, because of all the hassle and trustless environment.Blockchain pinpoints the problem and gives both parties an excellent, secure and trustworthy network, where everything is automated.

5.4 Notary Public : The authenticity of documents can be verified using Blockchain Technology by eliminating the need for centralizing authority. This could help in verification of 'Proof of Ownership of any asset', 'Proof of Existence of that asset' & 'Proof of Integrity of that asset' through the record of its documents stored in Blockchain. Using Blockchain for 'Notarization' independent of any third party secures the privacy as well as certification of the concerned document but these services are legally binding due to the fact of no involvement of any outside party. This service also eliminates unnecessary transferring fees of documents and thus saves resources. e.g. Viacoin, Crypto Public Notary and Ascribe are a few companies to provide notarization services through Blockchain Technology.

5.5 Music Industry : Reach of internet and access to number of streaming services has grown exponentially in the past decade and so does the music industry along with them. This change in the music industry has impacted everyone, including artists, labels, publishers, songwriters and the streaming service providers. The process of determining the royalties has been a real complicated one since the beginning and the emergence of the internet has made it even more complicated due to increase in maintaining transparency of royalty payments by both the artists and songwriters. The Blockchain technology can be really helpful in maintaining a comprehensive and accurate distributed database of the music rights ownership in the public ledger. By adding to the ownership information to the public ledger, the royalty split for each work can be recorded by smart contracts and added to the database.

5.6 Decentralized proof of existing documents: Traditional validation of authenticity of documents relies on central authority which presents some obvious security challenges. This system becomes more competitive as the documents gets older. The Blockchain Technology provides a better and secure substitute to this traditional proof-of-existence of legal documents. Blockchain provides a simple service to anonymously and securely store proof of existence of documents. A cryptographic digest of the file linked to the document is stored securely on the system. So, it is the cryptographic digest that is stored but not the actual document which protects the ownership of document which allows the user to anytime certify the very existence of document. The major advantage of this service is security which doesn't allow any third party to alter the documents.

5.7 Decentralized IoT: Internet of Things (IoT) is a big thing that's becoming popular in both consumer and enterprise space. Majority of Iot platforms are dependent on a central authority for its operations. This approach has specifically lead towards decentralized Iot platforms. The Blockchain technology has lead to secured and trusted data exchanges between devices by facilitating decentralized Iot platforms. e.g. IBM in partnership with Samsung has developed ADEPT, a platform to build distributed network of devices that uses Bitcoin underlying

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

technology's elements that allows decentralized file sharing, Smart Contracts and peer-to-peer Messaging.

5.8 Change the way we Vote: Blockchain accessibility and integrity can change the way we cast our vote. Blockchain fundamentals like immutability, accountability and security drives the potential for securely voting protocol. Using this system, every individual's voting data is inputted into blocks that are time stamped, encrypted and then 'locked' to avoid tampering with them. The information can't be altered due to distributed ledger technology and hence ensuring that all the data is copied on nodes across the network. There is almost nil probability of information being lost or database deletion and thus protection data locked in each block. This not makes elections safer to run also makes them cheaper and easier to run with wide access to voters through online means.

6. Conclusion: The paper has demonstrated various concepts of Blockchain Technology which might be expansible to a variety of situations. The mentioned features are not limited to the context of currency and payments only but also to contracts, property and beyond to government, science, publishing, art and culture and probably even to a much larger scale human progress. Like any technological advancement in history, this technology too disrupts initially but over time, this could help in the development of a much larger ecosystem which proves decentralized economy complementary to the centralized one, this could build an ecosystem which includes both fiat and crypto-currencies existing in the economy side by side. Certainly, blockchain is an Information Technology (IT), but beside IT, it comprises a lot of other things, digital currency based on blockchain technology has proved to be an embedded economic layer that the web never had. Basically, offering decentralized governance services is what Blockchain does. It could provide the exact number of documents with the exact amount of content of any document once uploaded to the system at any point of time. The technology integrates human-machine interaction, Internet of Things (Iot) usage and also Machine –to-Machine interaction. It is a public ledger which is independent of any third party (Decentralized system) used for registration, acknowledgement and transfer all resources and societal interactions, a public record, and a system to facilitate human progress in an unimagined way.

7. References

1. Asaph Azaria, A. E. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. 6.

2. Cosset, D. (2018). *Blockchain: What is Mining?* France.

3. Devan, R. T. (n.d.). Blockchain, A technical primer. 10.

4. Filippi, P. d. (2016). Blockchain-based Crowdfunding: what impact on. 11.

5. Fortney, L. (2019). *Bitcoin Mining, Explained.*

6. Frankenfield, J. (2018). Block Header (Cryptocurrency).

7. Friorik P. Hjalmarsson, G. K. (2018). Blockchain-Based E-Voting System.

8. Guy Zyskind, O. N. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *Institute of Electrical and Electronic Engineers*.

ISSN: 0971-1260
Vol-22-Issue-4-October-December-2019

9. Jesse Yli-Huumo, D. K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review.

10. Juroweic, P. (2018). Blockchain Applications In Insurance.

11. Lakhani, M. I. (2017). The truth about Blockchain. *Harvard Business review*, 11.

12. Lee, J.-H. (2017). BIDaaS: Blockchain based ID as a Service.

13. Lee, L. (2016). New Kids on the Blockchain: How Bitcoin Technology Could Reinvent the Stock Market.

14. Michael Crosby, N. P. (2016). Blockchain technology: Beyond Bitcoin. *Berkley*, 16.

15. Moutaouakil, P. A.-K. (n.d.). Blockchain, a catalyst for new approaches in insurance.

16. Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System.

17. S., J. (2018). *Blockchain: how mining works and transactions are processed in seven steps.*

18. Sagiv, M. (n.d.). The Blockchain Technology. 43.

19. Sin Kuang Lo, Y. C. (2017). Evaluating Suitability of Applying Blockchain.

20. Swan, M. (2015). *Blockchain: Blueprint for a new economy.* United States of America: O' Reilly Media, Inc.

21. Walker, G. (n.d.). Learn me a bitcoin.

22. Witold Nowiński, M. K. (2017). How Can Blockchain Technology Disrupt the Existing Business Models? .

23. Zibin Zheng, S. X. (2018). Blockchain challenges and opportunities: a survey. *IJWGS.*

24. Zibin Zheng, S. X.-N. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.

25. Zibin Zheng, S. X.-N. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.

