International Journal of Research in Engineering, Science and Management
Volume-3, Issue-5, May-2020
www.ijresm.com | ISSN (Online): 2581-5792

A Review On Blockchain

Abhijit[1*], Pragya Kapila[2]
[1,2]*B.Tech. Student, PDM University, New Delhi, India*
*Corresponding author: aromal76prasad@gmail.com

***Abstract*: Block-chain is a hyper distributed ledger which is adopted for decentralized transaction and data management. Block-chain is contemporary and powerful technology with a strong impact on the future for exchanging information and digital currency globally. We present a systematic literature review on block-chaining technology by reviewing the case proposed by the research community. Based on the systematic review and analysis we provide a comprehensive classification of block-chain and it's current scenario on the present world. We also glance to the future extension of block-chain technology as well as the particular limitation also. The article provides a paradigmatic view of three primary topics. First, some of the primary topics being discussed in regard to block-chain technology. Second, the representative view on the current scenario. Third, the potential future of block-chain development along with its impact on society and limitations of the block-chain technology and how these limitations spawn across various sectors and industries.**

***Keywords*: Blockchain, Distributed ledger, Bitcoin, Industries, Transaction.**

1. Introduction

Block-chain is quite new and interesting topic. According to Wikipedia a block-chain is "a continuously growing list of records, called blocks which are linked and secured using cryptography" (Wikipedia & Contributors, 2018b). In this article, we will identify a paradigmatic overview of current themes in block-chain research, discuss future implications and limitation. It is well understood, that it is growing rapidly, and really a scorching topic in current media also.

In this paper we will be providing an overview of current themes in academic publications and considering three main questions in regard to block-chain. We start with the question "what block-chain is" i.e. block-chain Overview. We then illustrate the application of block-chain in various field and industries such as in health-care, banking, cyber security, real estate, so on.

2. Blockchain Overview

We target to answer the following query in depth. What is block-chain? According to various resources Block-chain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008. The intention of this technology is to serve as the public transaction ledger of the crypto currency bit-coin. According to MELANIE SWAM (2015). "The block-chain is seen as the main technological innovation for Bitcoin because it stands as a "trustless" proof mechanism of all the transactions on the network" [1] .This public distributed ledger system maintain the integrity of transaction data and data management. Since the day of old ledger system where people recorded the exchange of goods and services as we in the digital age and using such old centralized ledger system recording such transaction has become much more complex. So because of the growth of global trading and commerce has created a distributed ledger system which is secure to fraud, error and misinterpretation. A block-chain records every sequence of transactions from beginning to end whether it is an online payment or hundred business transactions as each transaction proceeds, it put into a block and each block is connected to one before and after it. These blocks are grouped together and in this database each block records the data has been encrypted and given a specific identifier called the hash, each hash of the block is added to next block depending on the hash of previous block that creates a indestructible chain. It can trace goods path from the producer to consumer's hand with exceptional security and transparency.

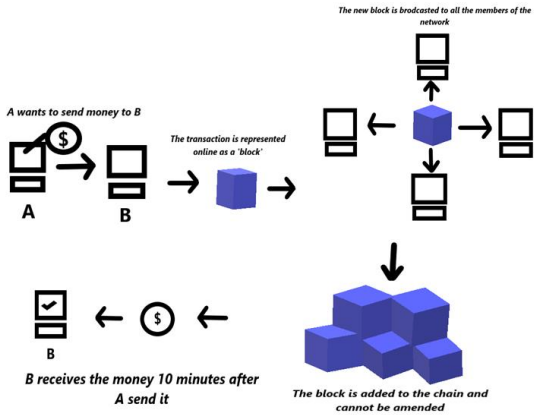

Fig. 1. Overview of blockchain technology

There are three key features that make the ledger block-chain efficiently capable to handle the requirements of person or organization:

- Distributed
- Permission
- Secure

Block-chain is a distributed ledger that permits the data to be recorded globally on chain of blocks, which allow anyone on the network to check everyone else entries. That makes it impossible for any user to gain control of the network or system.

Everyone in the network is permissioned to have the copy of detail and record and no block can be added in between the block which making it temper resistant and highly secure which deals with fraud and errors. Let us take an example, in the gold exporting the block-chain ledger keeps the photo of each gold and providing the certificate of authenticity, payment transactions as well as the product detail such as color carat and gold identity number and no one can temper with it. Block-chain technology works to create a permanent and secure database that makes block-chain capable for the storage of a record and transaction that involves value or in other words need to be secure and these distributed records are called distributed ledger. Here's an example, suppose there is a conflict between Mike and Ellen that who owns the precious diamond which is been in their family for years. As we see the ledger method is used in the block-chain, there was an entry in the ledger, display that Johnson owned the diamond in 1895 and when Johnson sold that diamond to Steve new block is added to the ledger which records the transaction between the Johnson and Steve. Every time a new ownership to this diamond is record in the ledger, until mike bought it from his father in 2007 that means mike the current owner of the diamond that can be shown in the history in the ledger. According to Narayan Prusty (2017). "Decentralized applications are fault tolerant as there is no single point of failure because they are distributed by default" [2].

Peer to Peer network which is an essential part to the Block-chain technology also referred as P2P network. The current generation uses the centralized client server form of network often operated by a organization and this organization handle all the request and requirement on the network and store all the information i.e. a central powerhouse storing and managing the information. "A crypto currency is a purely decentralized peer-to-peer electronic cash system, and is the first technology to successfully overcome the requirement for a centralized party to validate transactions" [5]. On account of this centralized network there is a serious condition arise that is all the sensitive and private data can be tempered and the user have almost no control over how their information is exploited. Therefore, the Block-chain is far better than the tradition client-server network because there is no central authority i.e. the third party who store the information and controls it. Instead there all the information on the network is recorded and transferred in between the participants on the network and these participant is known as peer who records the identical copies of the network, that's why it is called Peer to Peer network or P2P network.

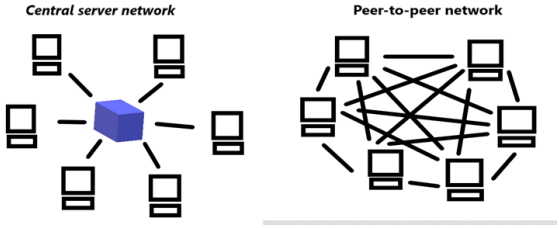

Fig. 2. Server and Peer network

The block-chain is not a single network and it can be implemented in three different ways.

1. Public Block-chains: Some block-chain can be fully public that is it can be accessible and open to everyone to access and view.
2. Private Block-chains: Some other block-chain is accessible by only authorized group of users such as a company, group of banks and so on.
3. Hybrid Public-Private Block-chains: In these block-chains, those who have private access can see the data while public are provided with list of selected data. 4. On other hand, every person is provided with all data but only selected users have access to add new data.

Block-chain technology has created to a new platform for business relationships that combines ease of use at low cost and high security.

The Proof of Work (PoW) which originally dated back to 1993 and this concept is used to prevent denial service attack. After 16 years i.e. in 2009 the Bitcoin establish the proof of work in an innovative way as a consensus algorithm which is used to validate transaction and build new block in block chain. Proof of work is not the efficient method but it is widely used across globally. In brief, the block-chain based system such as Bit-coin are maintained by effective work of decentralized node i.e. peer. Some of the nodes are known as miner which are responsible for adding new block to the chain. Here individual or group of miners are given with a puzzle and who solved it first will able broadcast it and other miner will verify it i.e. the miner need to find the nonce which then combined with the relative data and passed through the hash function and must produce the result which need to be matched with the condition. When the suitable result is found then other miner will confirm the outcome and miner will be rewarded. This means that it is impossible to add new block in the chain without finding the valid nonce which is used to create hash to the new block. Proof of work helps to counter the numerous service attack. But the issue with the proof of work is that expensive computer hardware is required for mining which consumes large amount of power the Sothearath SEANG proposed that "PoW system can be attacked if a miner alone or a collusion of miners who possess more than half of the network total mining power. This is also known as the 51% attack" [8].

3. Codification of Real-Time Blockchain based Application

Block-chain technology is the one of the biggest innovation where more and more people are understanding that decentralization and transparency attracts multiple industries.

A. Food Industry

As we see many big shopping and food industries are involving the block-chain in their food management system. We need to understand that, what happen if the block-chain is implemented to maintain food records, remember that block-chain is a open ledger and in which data in it is open to everyone

therefore there no authority that storing the records which a biggest advantage for consumers to track the origin of what they are buying, for example from the moment the carrot is harvested from the farm to when it was laid out on the market counter, you can see the detail when it is harvested , when carrot reached the counter and how long it's been in the store. The biggest shopping industry WALMART has already done two test runs with IBM using the hyper ledger fabric which is built by IBM. It is amazing that the vice president of the WALMART said in the interview that "We were so encouraged that we really quickly started reaching out of other suppliers and retailers. There is a big impact as block chain is integrated into food industry it will make the whole process more secure and there is more lead to a transparent block-chain on the food system that is all the consumers are provided with where and when each item of the food came from then there will be no risk of getting the old or unsafe food which make a better bond with the consumer." Supporting the technology as part of the general goals of optimizing the competitiveness and ensuring the sustainability of the agri-food supply chain" [4].

B. Real Estate

Real estate is incredibly complex because it is time-consuming, complicated, risk-taking as well as it is expensive. Let us see why real-estate is intricate, real estate agents, home inspector, government agents, everyone need to check and sign off on your payment or transaction and all of them will take the commission from it. Therefore, block-chain technology can create the process of purchasing and selling of land in real estate much easier and trouble free. When you wish to buy a land, there will be rules that seems difficult to deal because it depends on what type of property you are willing to buy and where do you want to buy i.e. which city, country or state and how to buy which need a third party or multiple middle men which take or pay the commission from your transaction. To avoid this problem, block-chain need to be implemented which plays an crucial role, if we add all the local, provincial and national housing rules and regulation into the block-chain this makes the dealing extremely simplify i.e. a prospective client simply provide the location, the budget and some other information then pulls the database to see the convenient location for the prospective user and the buyer can meet with the seller agreeing for price and send their digital signature to confirm their purchase and update all the documents as required. And the property need to clearly and securely register in the block-chain to make easy and ensure the transfer of the ownership. In a survey, from 2012-2013 New Delhi alone had approximate 181 reported cases of property fraud and similarly with the Mumbai having 173 cases, to counter this issue they put the land registry on the block-chain by introduction the cryptographically secure digital fingerprint.

C. Cyber Security

Due to the centralized system the current network of internet is vulnerable to cyber security which causes fraud and data theft. The Bank of England said: "There is more than one way in which a distributed ledger system can work, and remuneration would have to be designed in such a way as to incentivize honest participation in the system without leading to socially inefficient over-investment in transaction verification" [3]. Let's imagine a scenario, Rohan is sending Rs. 2000 to Ravi, So Rohan sends this money and the transaction detail are stored in the central authority's cloud. Now what if a hacker tries to hack the data within the cloud and tampers it, he/she successfully complete the mission and he receives the Rs. 2000 instead of Ravi. Therefore, cyber-attack are the major threat to the banking and other system. Where Block-chain is the best counter to protect our information and sensitive data from tampering as well as improving the cyber security across all industries. Let's take the same plot but with the aid of block-chain/ bit-coin, now Rohan send 0.00451 BTC to Ravi and block-chain which is a hyper distributed ledger which distributes the transaction data across multiple peers within the network and secures this information using cryptography by sending a copy of the network to each node which make the hacker impossible to hack it (i.e. if hacker try to hack the distributed system he/she is unsuccessful because of the peer to peer network or P2P network which make impossible to tamper with the data), now Ravi receives the money within 10 minutes without any problem. The real-life example is Citibank said that" block-chain technology is more seen as a complement to existing network". The impact will be more from its ability to open up new markets and helps to reach new customers in future.

D. Healthcare

This is the one of the major field where block-chain plays an important role and have a great potential in this field. The main benefit of the block-chain technology in health-care field is to increase the accuracy of EHRs (Electronic Health Records). The very important part is to store medical data of the patient which is a sensitive data which can be tampered. So exchange of medical report and data can be done securely by decentralized network in block-chain technology. If any patient needs to make personal medical data, the most suitable type of block-chain would be private block chain. The Würst and Gervais proposed, "a block-chain can be used in a scenario where multiple parties who do not trust each other need to interact and exchange common data, but would not like to involve a trusted third-party" [9]. The current health-care infrastructure depends on the trusted third party but in many cases these can't be fully trusted. As block-chain doesn't need any central authority and also relies on the consensus which easily solve this problem. There are many other health care areas where block-chain makes a big influence such as money transaction i.e. medical billing, provider credentials, medical record exchange, drug stock, etc. these systems also help merge patient data, enables medical records exchange across different health-care institutions.

E. Digital Voting

Voting is the most important part of a country which makes government for the people, to the people and by the people. In the current scenario, voting is conducted on paper or on the special electronic devices such as EVM [Electronic Voting Machine] and both have their own problem i.e. voting on paper cost lot of money and electronic voting have security issue. Recently, some country such as USA moves to ballot paper from the electronic voting because they feel safer in using paper ballots as compared to electronic voting machines. Instead of all of these, we can use block-chain to toss and store vote. One of the features of block-chain is the transparency, which make the system transparent to every voter that helps to verify the voting count for themselves and make the tampering impossible to perform. "The first use of block-chain voting technology happened in Denmark when the Danish Liberal Alliance used a block-chain voting system to conduct an internal vote in April 2014 during its annual meeting" [6] . There are some challenges to implement it which makes it a tough nut to crack. Firstly, we have to identify the voter and put it into the block-chain without leaking their privacy detail. Secondly, if we are allowing the voter to vote from their respective devices then we have to ensure that there will be no malware with tamper the voting process. Last but not the least the security, it is need to be seal with the denial of service attack with make all the progress unusable. If this idea become reality, then it could make more transparent and more convenient voting system as Columbia is do tests to implement it.

4. Open Issues in Block-chain Implementation

"Block-chain technology is still in testing phase and its implementation has some issues that have to be addressed when trying to establish Block-chain free cryptographically secured system" [7]. Like any other emerging technology there will be issues and challenges which may be arise. We will discuss some of the issue in following way:

1. Performance issue: The current problem with the block-chain system for bit-coin is that it takes 10 minutes to clear and settle a single transaction or Ethereum that takes 15 seconds i.e. it processes 3 to 20 transactions per second (tps). In contrast VISA transaction network can process 2000 tps and Master-card transaction network can process 5000 tps. That's why bit-coin won't displace Visa or Master-card soon.
2. Latency issue: The word latency in network is referred as "block time", that means the time required to create the next block of transaction in the chain. For example, the amount of time a client has to wait, after pressing the "send" transaction button and to see their transaction appear on the block chain or not. But VISA and Master-card transaction process takes seconds at most.

BITCOIN	600 sec
LITECOIN	150sec
NEO	21sec
ETHEREUM	15sec

3. Security issues: As we know as block chain has its own security benefit because it is a decentralized system. Nobody can make any changes to the ledger on account of the ledger is public. Although security issues may rises. According to Satoshi Nakamoto "when an individual or a group has more than 50% of the mining power, it is 51 percent attack". Due to this attack the old miner are not able to make new block and prevents from making any transaction although. To counter this issue, mining pool needs monitoring at all time.
4. Cost issues: The block chain technology is quite cost reduction i.e. in real estate, banking. But still there are some challenges regarding to implement this efficient system. The initial buildup of block-chain infrastructure is expensive. Small scale companies and banks wouldn't prefer to invest in block-chain that doesn't hold a profitable and promising future. And there are many factor contributes in high maintenance cost.
5. Scalability: Block chain technology is a central attraction many industries such as financial industry. Block-chain is still an emerging technology which is not capable of handling the large number of financial transactions that occurs each day. The leading block-chain networks have encountered a decrease in transaction speed and increased fee per transaction.

5. Conclusion

This technology in current scenario plays a crucial role in different industries or in data mining. As in the paper block-chain is decentralize database where numerous node i.e. computers across the globe are connected. Because of the decentralize ledger, it is difficult to tamper and remove data from the block. Mining backups the data in the decentral network making distributed ledger technology transparent. The block-chain technology ensures that every node have the copy of the detail and transaction of the network. At the same time this networks are available for inspection of complete information history which can be follow back to when some part of information was created. Because of the various factors like hashing, distributed ledger, decentralize network, immutability and so on makes the block-chain technology unique which makes my industries to adopt it. Block-chain is considered as the secure network technology, because of the distributed ledger and the peer to peer network. This technology is best source for the future research world. There are some issues which will try to overcome in upcoming time.

References

[1] Melanie Swan (2015), Block chain Blueprint for New Economy.
[2] Narayan Prusty (2017), Building Block chain Projects.
[3] Ian Allison (2017), Bank of England: Central bank looking at hybrid system using bit coin block chain technology.
[4] Andreas Kamilaris, Agusti Fonts, The Rise of Blockchain Technology in Agriculture and Food Supply Chains.

[5] Jeff Herbert, Alan Litchfield, A Novel Method for Decentralized Peer-to-Peer Software License Validation using Crypto Currency Blockchain Technology.
[6] Bogdan, Diana (2016), Democratic and Efficient: Is Block chain voting Our Future?
[7] Bojana Koteska, Elena Karafiloski and Anastas Mishev, Block chain Implementation Quality Challenges.
[8] Sothearath Sean and Dominique Torre (2018), Proof of Work and Proof of Stake consensus protocols.
[9] Marko Holbl, Marko Kompara (2018), A Systematic Review of the Use of Block-chain in Health-care.