Advent Of Disruptive Technologies – Assimilation Of Block Chain And Iot And It's Challenges In Relevance For The Upliftment Of Digital Relationship

H.Muthukrishnan

Abstract : In recent days, Internet of Things has occupied majority of places like industrial automation, smart homes with the advancement of mobile technology. Through which we have the control over all the electronic devices and home appliances. By which, everything can be controlled with our mobile phone. There by, its application and utilization has boosted to great extent irrespective to smart home appliances. Industrial automation has driven this field to all possible places to sense the environmental surroundings not limited to agriculture, automobile industry. Possibly in all fields. However, it has generated plenty of data, which has to be analyzed. Whenever data is involved in any research, it has to be secured. Disruptive technologies like big data and cloud computing has been enlightened to address the data security seriously. This paper addresses and interpolates the challenges in securing data generated by sensors. As, these data are sent and stored in cloud storage.

Index Terms: Block chain, Data security, Trust, Cryptocurrency, Distributed Ledger Technology, Bit coins, Privacy, Identity Management, Mining, Consensus

1. INTRODUCTION

Due to evolution in chips and chipsets large sized processors and sensors were reduced to compact micro mini electronic devices. This miniatures and wireless technologies has elevated the advancements in our society. There is a rapid growth in number of electronic devices in all areas of application where it can be suitably utilized and there is a complete drift in the production cost and toppled this real world into the world of digital communication. Eventually, there falls the conversion in communication from wireless networks to radio frequency Identification (RFID)[1]. Now, IoT had connected the whole world with various devices most of them wearable technologies. Various industries have incorporated the smart applications like smart home, wearable devices, smart cities, Health care, Automotive industry, smart agriculture, smart grid etc. Characteristics of this application which involves IoT are very peculiar as it generates huge volume of data with considerable amount power consumption with limited memory and storage. It creates an adorable question for all the researchers, towards unquestionable doubt over the data security, data reliability and trustability. Always, there exists the possibility of tampering data. Data can be altered, modified by anonymous person for the personal benefit. Only possible way to provide security to the sensor generated data is decentralizing. In the sense, the data has to be distributed over many devices which participate in the eve of communication. Data tampering can be avoided. Distributed Ledger Technology provides and supports reliability over data and its trustability. This technique can elevate the existing process in all fields which involves data of huge sizes like big data, fast data etc. Distributed Ledger technology s a digital system for recording the transactions like who initiated the data transaction, timestamp, with whom it was communicated wiz. In multiple places at the same time. Bit coin is the first solvent which potentially used in cryptocurrency for data reliability. Hereby there created and coined a name called block chain. Cryptocurrencies illustrates many significances of Block chain.

In this paper, we analyze the efficient merits and opportunities of IoT and Block chain.

Contributions are:

1. Blockchain, architecture and its working
2. Features of block chain technology
3. Assimilating IoT and Block chain.
4. Challenges in IoT – Blockchain assimilation
5. Conclusion and future works

2. BLOCKCHAIN

Block chain can be considered as a distributed append only timestamped data structure. Blockchain is digital, decentralized technology which maintains a record of all the transactions which happens over a peer-to-peer network. However non-trusted members communicate with each other without the need for trusted authority unlike digital certificates. The records would be stored in decentralized systems which are interconnected. Blockchains are "tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company or government). It facilitates a set on interconnected mechanisms to supply peculiar features to the infrastructure. The empowerment of blockchain innovates the "production of a decentralized domain, where the cryptographically approved exchanges and information are not under the control of any outsider association". Any exchange at any point finished is recorded in an unchanging record in a certain, safe, straightforward and perpetual way, with a timestamp and different subtleties [2] The corporate offices which uses blockchain to record data were allowed to store data in the some of prescribed types.

They are:

- Identity management
- Medical transaction records
- General documentation
- Management Activities
- Transactions

3. BLOCKCHAIN ARCHITECTURE

It is a closed Network of systems which are connected to a centralized server mechanism but not with the network which are mutually connected. Systems in this type of network accepts shared Data to some limitations forced on the Data. We use signed transactions between the peers at the lowest level of this existing architecture. These transactions express an agreement between two participants, which involves the transfer of physical or digital assets. The involved transactions should be signed or authorized at least by one participant and the same has to be distributed to all the participants or neighbors. The participant or entity which connects the block chain are called nodes. Nodes, which verifies and validates the rules are called full nodes. The distributed state is simply a shared state machine, with each block designing a modification to the updated distributed state. In this distributed state, nodes will aggregate the transactions into blocks which are responsible in validating the transactions. Mainly blockchain architecture contains Transactions, blocks, mining and consensus. Consequently, Architecture of Blockchain includes so many Factors.

3.1 Transactions

In fact, the purpose of blockchain will always stick to transactions. They are known as Tiny Building Blocks of Blockchain online training system. Transactions will have the Address of sender, address of Recipient and a value. This is indifferentiable from an original transaction, which we may see on a Credit card statements. A Bitcoin process [3] will also consist transactions. Each and every transactions of the Bitcoin will transfer the value of other bitcoin from single address to another address. The position of accepted correct block chain can be altered by transactions. A blockchain is a Shared State Machine. It meant that every node catches own copy of block chain. Incidentally, the updated state defined by, processing as a result of, every transaction in order as it shows in architecture of block chain.

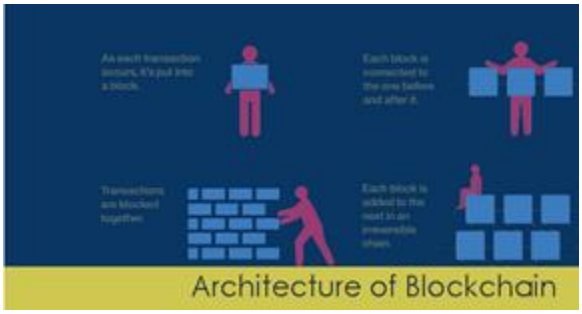

Fig. 1. *Blockchain Architecture*

3.2 Blocks

Generally, Blocks are Data Structures a kind of linked list. Their purpose is to bind so many sets of transactions and distribute it to every Node in the Network. Blocks are designed by Miners. Blocks has a block header, known as Metadata that helps to verify the Duration of a block. Block Metadata possess the current version of the design. Past block header hash and preferred block is parent block. Merkle root hash, a cryptographic hash for every transaction contained in this block.

3.3 Mining

Mining real and practical work to design true block that will be accepted by end of the Network. Consequently, miners are equal to the making of the network of the credit card company. They keep transactions pending and cryptographic. make them to be placed on the block chain. Hashing functions have good properties that make them design proof of work. Therefore, the transactions must be kept in blockchain to guarantee that there will be no corrupted branches and divergences. This is the goal of consensus layer. There exist various categories of consensus mechanisms based on blockchain type. Very well-established mechanism is Proof-of-Work (PoW). Complicated computational processes will be solved with hashes with specific patterns like number of leading zeros for ensuring authentication and verifiability. Proportionately splitting the blocks relative to the hash rate of miners, Proof-of-State (PoS) [4] protocol splits the block proportional to the wealth of the miners. This way selection is fairer and domination of wealthy participant will be eradicated. So, many blockchains like Ethereum are slightly moving towards PoS due to its minimal power consumption and improved scalability. Another consensus approach includes Byzantine Fault Tolerance(BFT) and its variants.

4. WORKING PRINCIPLE

Every new record or exchange inside the blockchain suggests the structure of another block. Each record is then examined and carefully marked to guarantee its validity. Before it is added to the system, it ought to be checked by most of hubs in the framework.

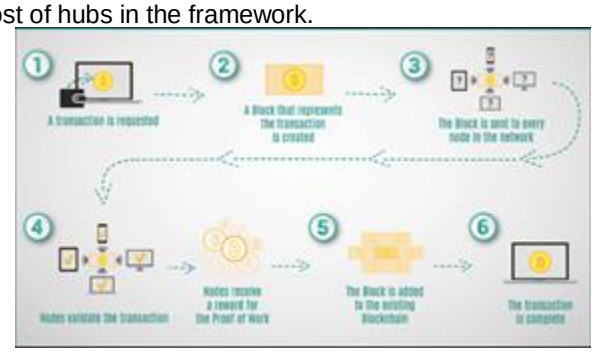

***Fig. 2**. How it works?*

Blockchain block consists of:

- certain data
- the hash of the block
- the hash from the previous block

The information packed inside each block relies upon the sort of blockchain. For instance, in the Bitcoin blockchain structure, the block keeps up information about the collector, sender, and the amount of coins. A hash resembles a unique mark (long record comprising of certain digits and letters). Each block hash is produced with the assistance of a cryptographic hash algorithm (SHA 256). Adjacently, it distinguishes each block in a blockchain structure effectively. Essentially expressed, hashes help to recognize any adjustments in blocks. The last component inside the block is the hash from a previous block. This makes a chain of blocks and is the principle component behind blockchain design's security. For instance, block 14 to block 15. The absolute first block in a chain is somewhat

exceptional - all affirmed and approved blocks are gotten from the beginning block. Any degenerate endeavors incite the blocks to change. All the accompanying blocks at that point convey wrong data and render the entire blockchain framework invalid. This blockchain operation can be supported by the network peers by providing the following functionality: routing, storage, Wallet services and mining [5]. These functions provide different types of nodes can be a part of the network.

5. FEATURES OF BLOCKCHAIN TECHNOLOGY

To fully understand the key features of blockchain, we need to first de-construct the hype and dive into the nuts and bolts. What exactly is a blockchain? Using blockchain to power cryptocurrencies is its first successful implementation. Features that make blockchain great for digital money and possibly many more applications. In short, we technically call blockchain is cryptographically hashed linked list [8]. Let's break it down.

5.1 Blockchain as a data structure

It's is a growing record of data, compiled as virtual blocks. In Bitcoin's blockchain, the data being recorded is Bitcoin transactions. The structure starts with a single block, known as the genesis block. As the amount of data recorded on the system increases, more blocks keep getting added. Each block in the sequence is linked to the previous block, going all the way back to the genesis block. This "chain" of blocks is what gives this type of data structure its clever name, which we discussed in the previous topics.

5.2 Immutability and tamper detection in blockchain

Data stored in the blockchain is made secure and immutable using cryptography. Every block is referenced by a unique string of characters, generated by a cryptographic hash function. This function can accept any amount of data as inputs and generate a fixed length string as output (hash). Each block in the chain carries the parent block's hash taking all the way to genesis block. Hence data tampering, in any block across the chain will subsequently alters the hash of other blocks as well. There by it ensures the identity tampering at any point of transaction. For this reason, we call this as a Distributed Ledger Technology. Everything will be recorded. Every modification will be entered and the same will be reflected in all the blocks.

5.3 Data protection in blockchain

Instead of a physical or online account that has to be maintained by a third party (such as a bank), every unit of bitcoin is stored on the blockchain itself. Accessing bitcoins securely for users can be achieved through their private/public key pairs. A consumer can spend or transfer his bitcoins only by using his private keys, while a merchant can receive bitcoins by sharing his public keys with the consumer. Once the transaction has been relayed throughout the internet and included in a block, it is considered permanent. The merchant can then irrefutably claim ownership of those bitcoins. He can also use his own private keys to spend those Bitcoins and so on. The blockchain is typically stored and maintained on multiple devices. Thousands of devices worldwide store the bitcoin blockchain. Thus, the data is protected even if one or more of the devices are compromised by an attack or network issues.

5.4 Distributed ledger technology

Perhaps the most popular attribute of the blockchain, the distributed ledger of data. The ledger can be shared among a private group of users connected through the local area network, or with millions across the internet. A message is relayed on every new block creation, to ensure that all users have a latest version of the ledger. This feature has applications well beyond digital currencies, as it eliminates the need of a trusted central party to record the information. Areas ripe for disruption through decentralization include stock exchanges, real estate transactions, personal identification and many more. Since the ledger is stored on multiple storage devices, possibly in different locations, it also protects the system from data loss in case any devices or servers face downtime. Other users can continue accessing and adding information on the blockchain, as long as there is at least one online device that has the latest version of the blockchain. With this upgraded feature, block chain trumps into the field of data security at greater level.

5.5 Blockchain's solution to double spending

Double spending is quite simply the risk that a user may spend the same units twice. This is a kind of sharing a message on any messenger (the ubiquitous messaging app) with several contacts. The receivers may not even be aware of how many others got the same message. While this is not a bug (it is in fact a feature) in messenger, it could spell disaster when transferring money or shares. If we could sell the same artwork or apartment to different buyers, that would render those assets effectively worthless. This is the reason we have authorized clearing houses to settle trades in the stock markets. An elegant solution has been found by implementing bitcoin in a decentralized ledger and a consensus mechanism, allowing users to vote on valid transactions to be added to the latest block. Once the block has been relayed across the network, anyone can verify if the user actually owns the coins that he/she wishes to spend.

6. ASSIMILATING IOT AND BLOCKCHAIN

As a part of digital era, IoT has transformed and optimize the manual processes into automation, almost in all industries. It has leveraged assimilation of IoT and blockchain. Over the last few years, cloud computing has extended its greatest support for IoT in storing data and provided necessary functionality for further data analysis [9]. This unaccustomed growth of IoT has introduced novel technologies to analyze, process the information, access and information sharing. The union of promising technologies like IoT and cloud computing has proven to be indispensable. Likewise, we acknowledge the huge potential of blockchain in revolutionizing the IoT. Blockchain can enhance the IoT by providing a trusted sharing service, where information is reliable and can be traceable. Data sources can be identified at any time and data remains immutable over time, increasing its security. As a further matter, in areas like smart cities and smart cars, sharing reliable data could favor the inclusion of new participants in the environs and contribute to elevate their services and their adoption. Consequently, the use of blockchain can

complement the IoT with reliable and secure information. More specifically, improvements that this integration can bring include (but are not limited to):

6.1 Decentralization and scalability
The technological shift from a centralized architecture to a P2P distributed one will remove central points of failures and bottlenecks [12]. It will also help prevent scenarios where a few powerful companies control the processing and storage of the information of a huge number of people. Other benefits that come with the de-centralization of the architecture are an improvement of the fault tolerance and system scalability.

6.2 Identity
Utilizing a common blockchain system, participants are able to identify every single device. Data provided and fed into the system is immutable and uniquely identifies actual data that was provided by a device. Additionally, blockchain can provide trusted distributed authentication and authorization of devices for IoT applications [12]. This would represent an enhancement in the IoT field and its participants.

6.3 Autonomy
Blockchain technology empowers next generation application features, making possible the development of smart autonomous assets and hardware as a service [12,13]. With blockchain, devices are capable of interacting with each other without the involvement of any servers. IoT applications could benefit from this functionality to provide device-agnostic and decoupled-applications.

6.4 Reliability
IoT information can remain immutable and distributed over time in blockchain [12]. Participants of the system are capable of verifying the authenticity of the data and have the certainty that they have not been tampered with. Furthermore, the technology enables sensor data trace-ability and accountability. Reliability is the key aspect of the blockchain to bring in the IoT.

6.5 Security
Information and communications can be secured if they are stored as transactions of the blockchain [14]. Blockchain can treat device message exchanges as trans-actions, validated by smart contracts, in this way securing communications between devices. Current secure standard-protocols used in the IoT can be optimized with the application of blockchain.

7. CHALLENGES IN IOT – BLOCKCHAIN ASSIMILATON

Incorporating blockchain with IoT is very challenging. Let's address some of them here below:

7.1 **Security**
With 22 per cent jump in cyberattacks on Internet of Things (IoT) deployments in the country, India was the most attacked nation in the IoT space last quarter, said a new report released here on August 10 2019, 8:21 PM IST. This was the second consecutive quarter that the country topped the cyber-attack victims list [15]. Smart cities, financial services and transportation sectors led the sectoral rankings in terms of the attacks, said the report titled "State of Internet of Things (IoT) Security". Among the 15 Indian cities from which data was gathered, Mumbai, New Delhi and Bengaluru are attracting the maximum number of cyberattacks, revealed the study by Bengaluru-headquartered telecom solutions provider Subex. The study identified over 2,550 unique malware samples in the country. Internet of Things (IoT) projects are being targeted at the proof of concept stages itself and many malware samples isolated showed a tendency to persist and listen to the network traffic. Increase in the number of attacks with geopolitical motivation is also a trend, the study reported. Thus, the increasing number of attacks on IoT networks, and their serious effects, make it even more necessary to create an IoT with more sophisticated security. Blockchain can ensure that data in the chain are immutable and can identify their transformations.

7.2 Storage Capacity and scalability
As a debatable point of discussion is storage and scalability, IoT has generated data in GBs nowadays. Reluctantly, blockchain appears to be unsuitable for this IoT applications. In fact, recent block chain technology can process only a limited number of transactions per second. Not all the stored data in IoT is taken for processing. Very few of them were assessed and analyzed. As per the surveys done so far in the field of interest, states many different techniques to filter, normalize and compress the IoT data were focused to reduce this alleviated challenge.

7.3 Anonymity and data privacy
It's very essential in addressing the prime problem of data privacy and anonymity. Since, IoT indulge in private and confidential data of individuals or firms. However, bitcoin application may guarantee anonymity problem. This is the place, where the ability to hide the identity of person sending personal data in wearable devices has to be addressed. The problem of data privacy is very transparent in all categories of blockchain. Protection of data and privacy is key challenge. Reliability and trust worthiness are another prominent challenge need to be addressed and the same can be alleviated through blockchain application. Furthermore, data privacy can be addressed legally with the law and regulations defined in various country. Blockchain has to adopted legally in all countries as a legal platform to ensure data privacy.

8. CONCLUSION
Always, there exists the great controversies generated by disruptive technologies around the world. There is a significant technological revolution in virtual currencies. Block chain takes front seat here to address these alleviations against data involved. It needs to guarantee security more significantly. This paper de constructed the hype over disruptive technologies and dived into the nuts and bolts of Block chain architecture and functionalities, features and analysis of salient challenges that assimilation of block chain and IoT should take up on shoulders to address first. As futuristic implementations expects block chain to up rise the IoT application across the various fields which needs its serious involvement. Key to taste the essence of success is to adopt the regulations to include

block chain and IoT aa part and parcel of any Government infrastructure. This would elevate the communication and interaction between government organizations and the corresponding citizens in the country. With the advent of block chain would make impossibilities possible by permitting people to secure digital relationships.

REFERENCES

[1] Ana Reyna, Christian Martin, Jamie Chen ,On Blockchain and its application with IoT challenges and opportunities, Future Generation Computer Systems.

[2] Dr. Balakrishnan Subramanian, A data science Foundation white paper, August 2019

[3] https://onlineitguru.com/blog/architecture-of-blockchain

[4] Fran casino et al., A systematic review of Blockchain based applications, Journal on Telematics and Informatics, November 2018.

[5] A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, Inc., 2014.

[6] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008. Available online:https://bitcoin.org/bitcoin.pdf. (Accessed 1 February 2018).

[7] Y.K. Al-Douri, V. Pangracious, M. Al-Doori, Artifical immune system using Genetic Algorithm and decision tree, in: 2016 International Conference on Bio-engineering for Smart Technologies (BioSMART), 2016, pp. 1–4. Dubai.

[8] https://thefintechway.com/6-key-features-of-blockchain/

[9] M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing, J. Netw. Comput. Appl. 67 (2016) 99–117.

[10] G. Karame, E. Androulaki, S. Capkun, Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin, IACR Cryptology ePrint Archive 2012 (248), 2012.

[11] Quorum Whitepaper, 2016. Available online:https://github.com/jpmorgan chase/quorumdocs/blob/master/Quorum%20Whitepaper%20v0.1.pdf.(Accessed 1 February 2018).

[12] P. Veena, S. Panikkar, S. Nair, P. Brody, Empowering the edge-practical insights on a decentralized internet of things, in: Empowering the Edge-Practical Insights on a Decentralized Internet of Things, vol. 17, IBM Institute for Business Value, 2015.

[13] Filament, 2017. Available online: https://filament.com/. (Accessed 1 February 2018).

[14] G. Prisco, Slock. It to introduce smart locks linked to smart ethereum con-tracts, decentralize the sharing economy, 2016. Available online: https:// bitcoinmagazine.com/articles/slock-it-to-introduce-smart-locks-linked-to-s mart-ethereum-contracts-decentralize-the-sharing-economy-1446746719/

[15] https://www.news18.com/news/tech/india-ranked-highest-in-iot-cybersecurity-attacks-last-quarter-report-2265951.html

Mr. Muthukrishnan H is an Assistant Professor of Information Technology at Kongu Engineering College, Perundurai, Erode. He has over 9 years of Teaching Experience. He is awarded Masters from Anna University, Chennai in June 2010. He is life member of CSI. He has published 6 International Journal and 6 National conference papers and organized 12 National Workshop. He is certified AWS solution Architect in the year 2017 and certified instructor in bigdata from big data university. Published a book on Cloud computing.