ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

Review on Decentralized Infrastructure, Types and Issues in Blockchain Technology

Srushti Vajir

Assistant Professor, Department of Computer Engineering, Parul Institute of Engineering & Technology- Diploma Studies, waghodiya, Vadodara, Gujarat, India

ABSTRACT: Blockchain technology is one of the most popular Technology. Due to its influence, lifestyle of many people has been changed.It has great influence in the area of business or industry. Although the decentralized infrasture of the blockchain technology may provide us real time services. Blockchain Technology is responsible for providing robustness and real time environment for transaction and e-commerce activities.The blockchain offers the benefits of decentralization therefore it eliminates the problem of single point failure. The benefits of decentralized infrastructure, concept and usage of blockchain, types of blockchain as well as the security issues and challenges behind this innovative technique is also an important topic that we need to concern.

KEYWORDS:IOT, Decentralized Infrastructure, Blockchain Technology, Structure of Blockchain, Working, Protocols, Security issues

I. INTRODUCTION

Blockchain technology can be use to enhance the basic services that are necessary in trade finance and transaction. Basically, blockchain relies on a decentralized Infrastructure, digitalized Formation and distributed ledger model. This Features is more robust and secure than the centralized infrastructure which are currently used. Blockchain technology responsible for maintain decentralized record of transactions. The distributed ledger will maintain a single master database. It keeps valuable and updated record of transactions being proceed in real time environment, back to the source point of a transaction. This procedure is also known as the provenance, which is requirement in trade finance, which allows financial organizations to review all transaction steps and reduce the risk of fraud. Decentralized infrastructure will allow to operates at any level of organizational hierarchy by authenticated users only. This decentralized feature eliminate the con named as “Single point failure” of centralized infrastructure. As central authority fails all connected devices will not able to transact or proceed. In simple terms, block chain technology is shared and open ledger that keeps record of transaction. Name “Blockchain” means system include continuously increasing block of data containing information related to the transactions. Due to Decentralized infrastructure data can be accessible to every authorized client where as manage by cluster of computers hence not owned by a single person.Centralized systems are problematic for their vulnerability, due to this problem single-point-of-failure (SPOF) is the biggest issue. On the other hand, decentralized systems implemented in a distributed manner suffer from the data synchronization issue [4]. Blockchain Technology was first used by Nakamoto to run the idea of Bitcoin which is used peer-to-peer trust-less Electronic Cash.

II. MOTIVATION AND RESEARCH CONCEPT

As illustrated by ITU [5], the Internet of Things (IoT) refers to the network of numerous physical objects connected to the Internet. Such devices will acquire information about the surrounding environment and will exchange data with other devices or platforms, thus enabling several new services. Privacy prevision is the main issue while data is proceeding by using IOT devices.Nowadays, data that we produced by using devices are processed and stored by “ centralized Internet companies ” , which is responsible of full control and management of all the clients. Although the

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

data are distributed (Share) among different servers of the company, there is a single point of control and access to them, that is the company which owns those servers [6]. Therefore, how to slove the problem of Single point of failure is the latest research issue in IOT environment.

III. RELATED WORK

There are related survey papers [10], [11], [12], [13]that covered different aspects of the blockchaintechnology. For example, a brief overview of block chain for bitcoin was discussed in [10] however, these surveys are very limited regarding detailed discussion on research `challenges in blockchain. Moreover, how peer-to-peer technologies are represented decentralized infrastructure and its benefits towards the blockchain technology [13].

IV. CONCEPT OF BLOCKCHAIN TECHNOLOGY

Blockchain technologies consisting of Mathematics, Cryptography, Policies, Algorithm and economic decentralized model. It is Responsible for combining peer-to-peer network utilizing distributed algorithm to solve traditional distributed database synchronize problem.
The blockchain technologies introduced of six key features.

1.Decentralized: It is the basic feature of blockchain,means that blockchain does not rely on centralized infrastructure the data cab be kept tracked, store and updateddistributedily.

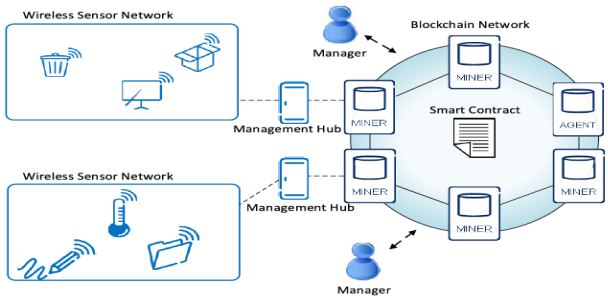

Diagram3.1: Decentralized Infrastructure [3]

1) Wireless Sensor Networks (WSN): It is a interactive network that provides constrained interaction in applications with limited light and power necessity.

2) Managers: This module is responsible to manage the access control permission and rights of a collection of Internet of Things devices. Generally, managers are said to be a lightweight node in IOT systems. Lightweight nodes are not responsible to store the blockchain data, information or recheck the blockchain's transactions.

3) Agent Node: The agent node will be considered as a typical blockchain node.This node is specific blockchain node which is responsible for deploying the smart contract. The agent node is the owner of the smart contract during the lifetime of the access control system [3]. If smart contract accepted into the blockchain infrastructure, then the agent node receives an address that locate the smart contract from the blockchain network. If nodes want to communicate with the smart contract, specific nodes in the blockchain infrastructure have to aware of smart contract's address.

4) Smart Contract: The access management system (AMS) ruled by the operations and functions defined in a single smart contract. This smart contract is unique and cannot be deleted from the system [3].

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

5) Blockchain Network: The blockchain network can be private blockchain for provision of simplicity and limit the users. The system can also use public blockchain to provide public access of all the node of the blockchain system. But the consortium blockchain is hybride and better option to choose.

6) Management Hubs: IoT devices do not belong to the blockchain network. Therefore, IOT devices required some power requirements and connectivity related requirements.

1.Transparency: Thedata'srecordbyblockchainsystemis transparent to each node, it also reflect the changes (modification) made by one node to another node connected to the network, therefore the blockchain can betrusted.

2.OpenSource Platform: Mostblockchainsystemisopentoeveryone, record can be reviewpublicly and people can also usethis technology to create any application theywant.

3.Autonomy: Becauseofthebaseofconsensus,everynode on the blockchain system can transfer or update data securely, the goal is to trust form single person to the wholesystem,andnoonecaninterveneit.

4.Immutable: Any records will be reserved forever, and can't be changed unless someone can take control morethan51%nodeinthesametime.Immutability refers to the fact that the blockchain is highly resistant to alterations. In the blockchain setup, the data blocks are linked and secured with a special cryptography technique, called hash.

For example, hash for —Good Morning is
E526F139218F16C1C65FC41ABE8B5B991769AE6718495A7AD9984406A54W2C.
And the hash for —Good Mornin is
511294185A8D2AD6A0C72EC63FF7D68F4C4AC538BD3256AFE21DE001WA22.

5.Anonymity: Blockchain technologies helped to solved the problem of trust between node to node, Hence the data transfer or even transaction can be anonymous, the requirement is only need to know the person's blockchain address.

6.Better Security: There is no central authority therefore no single point of failure to shutdown the network's communication. Most secure levels of financial system are vulnerable (affected) to hacks or intrusion. On the other side, Bitcoin system has never been hacked till now. It is quite possible to hack individual person's private keys if the key is not securely stored in repository, but the network provides security from its side otherwise.

V. WORKING OF BLOCKCHAIN

The working of blockchain algorithm is as follow:

1) The First node receives new data and broad casting to network.
2) The receiving node checked the message from those data which it received, if the message was correct then it will be stored to a block.
3) All receiving node in the network execute proof of work (PoW) or proof of stake (PoS) algorithm to the block.
4) The block will be stored into the chain after executing consensus algorithm, every node in the network admit this block and will continuously extend the chain base on this block.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

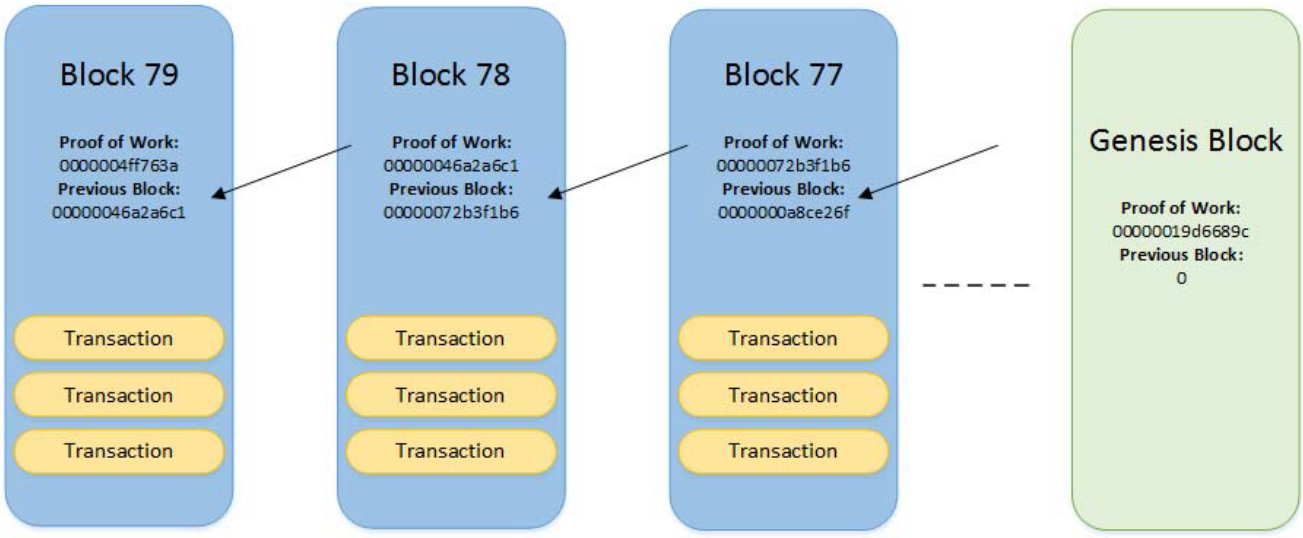

Diagram 4.1: working of block chain [3] [7]

VI. STRUCTURE OF BLOCK CHAIN

Blockchain consist oforiginal data,hash value ofprevious block, hash value of current block, timestamp and other information.

1.Main data Section: Main data section depending service on which this blockchain is applicable, for instance records related to transaction, bank clearing records, records related to contract or IOT data record.

2.Hash: When a transaction executed, it had been hashed to a code and then broadcast to eachnode. For the reason it could be contained thousands of transaction recordsineachnode'sblock. This technology uses Merkle tree function to calculate a final hash value. The final hash value will be stored in block header. This calculated hash value will be considered as a hash value for current block.

3.Timestamp. Time Stamp field indicate the time on which the block was generated.

4.OtherInformation: This field stores the data defined by the user. For examplesignatureoftheblock,Nonce value, or other data that userdefine.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

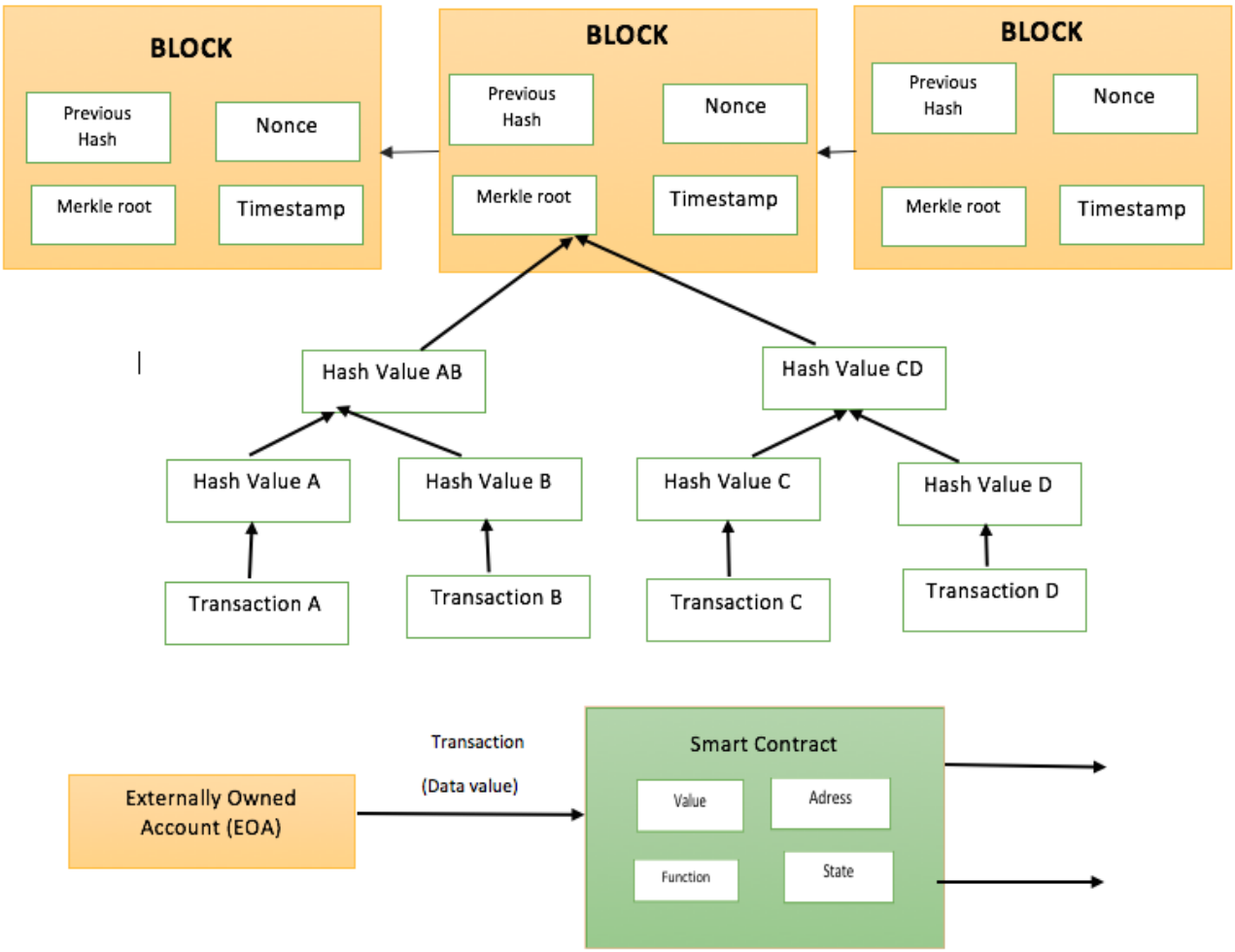

Diagram 5.1: Structure of Blockchain

VII. ALGORITHM OF BLOCKCHAIN

1. COMPARING PROOF OF WORK AND PROOF OF STAKE:

I have mentioned major blockchain protocol is Bitcoin. The bitcoin was introduced in November,2009. A thesis had been uploaded by Nakamoto on a US mailing list where the cryptographers share or exchange information. The title of thesis was “Bitcoin: A peer-to-peer electronic cash system” [2] which followed the mash topology that allows peer-to-peer communication (one-to-one) of each node on a network. Bitcoin’s public ledger—the blockchain—was first introducedin 2009 by Nakamoto [3]. Characteristics of this protocol:

1.Peer-to-Peer network allow to communicate or perform transaction directly. It does not required any trusted third party Authentication.
2.It provides non-reversible transaction system.
3.Casual transaction cause the credit cost, it can be eliminating by this technology.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

2. SOME IMPORTANT APPLICATION

2.1 Bitcoin: Bitcoin was the first blockchain to be conceptualized and implemented, and it is a crypto currency that serves as a digital financial asset. [3] Bitcoin is "Virtual currancy". But it also called crypto currency. It uses distributed technology while exploring the value in the data managed by software. The starting months of 2016 earned the issuance of approximately 15.26 million BTC, which is equal to around 7 billion US Dollars. Bitcoin system was design by using hash, digital signature, public-key cryptography, Peer-to-Peer and Proof of Work [2] [10]. This technology has composed a mechanism that prohibits duplication of payments and data falsification, additionally a mechanism that prevents unauthorized users, which are problematic for the operating system like the one for the electronic money, having no central authority.

2.2 Ethereum:Ethereum is a public, open-source and block chain supported decentralized computing protocol that provides smart contracts (scripting) concept [8]. The protocol has provided a decentralized virtual machine called the Ethereum Virtual Machine (EVM), which focus on Turning-complete scripts by using a global network of public nodes and the token called ether,is also referred to as gas. Gas is used for preventing the spam on networks and allocating the resources in proportion to the incentive provided by the request. Bloomberg explains Ethereum as publically shared software therefore it can be use by any people; Ethereum is used as a protocol(Set of Rules) for decentralized applications, smart contracts and decentralized autonomous institutes, with a number of functioning applications developed on it by March 2016, New York Times says[2].

VIII. TYPES OF BLOCKCHAIN

Blockchaintechnologiescan be divided into three parts:

1) **Public lockchains:**Everyonecanview and verifythetransaction, participants can also participate in the process of getting consensus. In this blockchain user can send, store and receives the data on the network of public blockchain after downloading the specific software according to service. This blockchain gives the permission of user to read, write and store data to the all public blockchain users. For instance, Ethereum and Bitcoin are both Public Blockchain. Figure shows public blockchain.

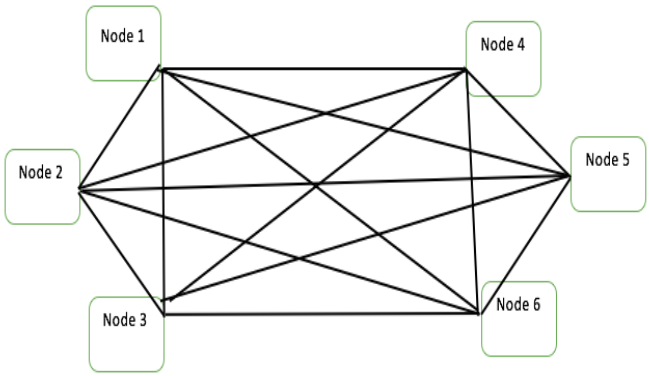

Diagram 7.1:Public blockchain

2) **Private blockchain:** In private blockchain node will be confined, not every node can take part in this blockchain, It has strict authority management on data access which are sensitive. In private blockchainread,write and send can be controlled by a single organization or company. That organization will establish set of Rules, Regulation and policies for the private users. As the

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

requirement of organization changed the set of rules and policies might be changed. Figures shows privateblockchain.

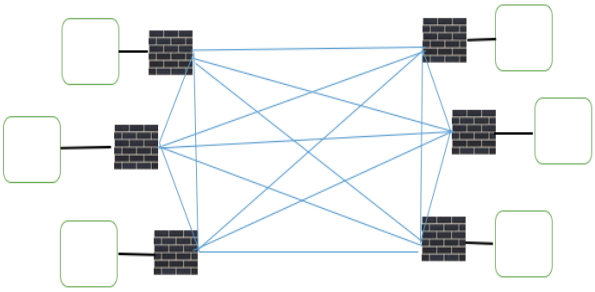

Diagram 7.2: Private Blockchain

3) **Consortiumblockchains:**Consortium bIockchain is a hybride method of Public blockchain and the private blockchain. It is called as a hybride model between low trust provided by the public blockchain and the single highly trusted model of private blockchain.Instead of allowing all users or allowing single organization to control the entire blockchain, this consortium blockchain will allow the selected parties to pre-determined. Itmeansthenumber of nodesthat had privillage (authority) can be select in advance, Consortium blockchain usually has collaboration like business to business, Open or private data can be supported by blockchain. This data can be seen as party is decentralized.R3CEV and Hyperledger both can be considered as the example of consortium blockchains. Figure shows consortiumblockchains.

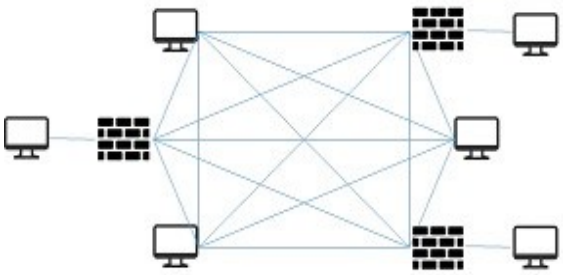

Diagram 7.3: Consortium Blockchain

Depending on a area where a person using block chain one of the type can be applicable. Each type has its advantages. Public blockchain is convenient where data needs to pass on and required less privacy management on that data. But, sometimes data should not be accessible to everybody rather it should be prevent from unauthorized access. Therefore, the Consortium or private blockchain are designed.

IX. SECURITY ISSUES AND CHALLENGES IN BLOCKCHAIN

THE MAJORITY ATTACK (51% ATTACKS) [2]

With Proof of Work, the prospect of mining a block is relay on the work done by the miner (e.g. CPU/GPUcycles spent checking hashes). Due to this methodology, people willing to co-operate in order to mining more blocks, and become mining pools", a repository where holding most computing power. At a time it hold 51% computing power, it can take

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

control this blockchain. Evidently, it cause security issues[9]. If some people is a owner of more than 51% computing power, the that person can find Nonce value quicker than others, meaning that person has right (authority) to decide which block is permissible.

What it can do is:
1) Altering the transaction data, it may cause double spending attack.
2) To prohit the block checking and verifying transaction.
3) To stop miner to mine any existing block.
A majority attack was more feasible in the past when most transactions were worth significantly more than the block reward and when the network hash rate was much lower and prone to reorganization with the advent of new mining technologies.

X. CONCLUSION

In this paper, I have compare compared three types of blockchain(public, private and consortium) and their benefits. Organization can choose one of this blockchain infrastructure according to their requirements.This Blockchain technology has many advantages like decentralized infrastructure, Real time environment, Removal of full control of organization on any activities, Fast online transaction as well as responsibility of work is distributed between participated nodes, therefore it is easy to locate the problem .In many cases, these benefits are worth those resources, which will be used to integrate it. However, there are also some disadvantage like fork problem is exist. To avoid that problem organization, need to match old and new agreement in compulsion as well as have to provide same computing power to both forks.

REFERENCES

[1]Iuon-Chang Lin1;2 and Tzu-Chun Liao2 –" A Survey of Blockchain Security Issues andChallenges" - International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017
[2]Sayani Chandra - "A Study On Blockchain Security Issues and Challenges" - 2018 IJNRD , Volume 3, ISSN: 2456-4184, Issue 5 May 2018
[3] Oscar Novo -"Blockchain Meets IoT: An Architecture forScalable Access Management in IoT"- IEEE Internet of Things Journal, VOL. 5, NO. 2, APRIL 2018
[4] WEI CAI, ZEHUA WANG, JASON B. ERNST –"Decentralized Applications: TheBlockchain-Empowered Software System"- August 22, 2018,IEEE Access.
[5] International Telecommunication Union, "Measuring the Information Society Report," International Telecommunication Union (ITU), Report, 2015.
[6] Marco Conoscenti, Antonio Vetro`, Juan Carlos De Martin-"Peer to Peer for Privacy and Decentralization in the Internet of Things" -IEEE/ACM 39th IEEE Conference on Software Engineering, 2017.
[7] Mohamed Amine Ferrag, MakhloufDerdour, Mithun Mukherjee, - "Blockchain Technologies for the Internet of Things:Research Issues and Challenges" – IEEE- 24 JUNE-2018.
[8] H. Watanabe, S. Fujimura, A.Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchainap- plied to smart contracts," IEEE International Conference on Consumer Electronics (ICCE'16), pp. 467–468, Jan. 2016
[9] N.T.CourtoisandL.Bahack,"Onsubversiveminer strategies and block withholding attack in bitcoin digitalcurrency,"*CoRR*,vol.abs/1402.1718,2014.
[10]Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A Blockchain based Truthful Incentive Mechanism for Distributed P2P Applications," IEEE Access, 2018.
[11]F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Commun. Surveys & Tut., vol. 18, no. 3, pp. 2084–2123, Mar. 2016.
[12]L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in Proc. IEEE 4th Int. Conf. on Advanced Comput. and Commun. Syst. (ICACCS), Jan. 2017.
[13] A. Kaushik, A. Choudhary, C. Ektare, D. Thomas, and S. Akram, "Blockchain-literature survey," in Proc. IEEE 2nd Int. Conf. Recent Trends in Electronics, Information & Communication Technology (RTEICT), May 2017.