REVIEW PAPER ON BLOCKCHAIN TECHNOLOGY

Rahul Paliwal,MCA Student,Uttaranchal University,Dehradun
Shubham Yadav,MCA Student,Uttaranchal University,Dehradun
Sameer Dev Sharma,Assistant Professor – Computer Application,Uttaranchal University,Dehradun

ABSTRACT

The blockchain can also termed as a digital coins field after all the evolution of bitcoins, bitcoin world's first and the largest cryptocurrency. It is used for the change nearly in every faces of our digital lives from the way we send money in the daily basis. By avoiding third forces blockchains promise to make our systems more efficient. By preventing restriction they promise to make our systems more equitable and if properly implemented they could make our systems more reliable and secure. So with the help of this paper we review the system of blockchain and its related applications with its advantages in real world in below sections.

Keywords: Blockchain,Cryptocurrency,Bitcoins.

INTRODUCTION

Software system architectural apporach can be illustrated into two categories[1] (i. Centralized) and (ii. Distributed).So the system which are categorised into the first apporach that is centralized software system are those where nodes are located in all places but they are connected with the main node that is called central node of organization, which will control all the nodes. But on the second approach the distributed system are connected to the many nodes but all the nodes are not connected to the central node.Here in (fig.1.[1])we can easily define the variation of these two apporaches of software system. We can say that there are several advantage through distributed system like by combining all the connected nodes we acquire more computing power, and then increasing the reliability of the nodes the system does not allow to a single failure of node in the system.But after having such powerful power it has several drawbacks which include communication raises and security issues thorugh which any unreliable network can harm the network and node in the distributed system. Meantime block chain technology implements distributed software system but we cannot say it completely work on distributed system rather we can say it works on inherently distributed system. Moreover block chain [2]

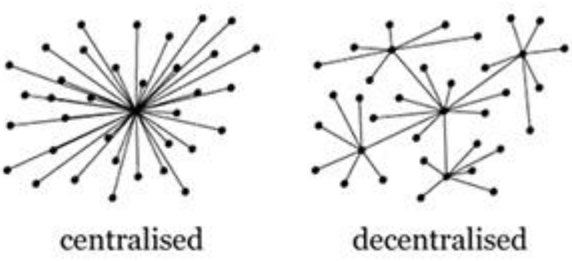


Fig.1

can also be treated as a pure peer to peer system,this peer to peer system is made up of all the individual nodes in a distributed system.Block chain is a decentralized system of secure and trusted distributed databases (distributed ledger). Which record and share the transaction details across with many nodes which are the part of the network so that the data can't be modified. The each transaction which held on the block chain network it is distributed across all the nodes on block chain each participant has a same copy of the ledger and it's a (immutable ledger) once the record or a transaction is recorded it can't be modified.In simple word we can term it as a chain of block that contain the information or transaction details it called a block chain.

Together with blockchain, Satoshi Nakamoto [3] invented Bitcoin that was originally as the first and most popular cryptocurrency.The centralized management system is not reliable for its users and also it doesn't provide a trustless and reliable transaction whereas through blockchain it enables trustworthy and reliable transaction to its users all the information are in the public domain. Thats why the blockchain is famous and acquiring lot of attention by implementing decentralized system into transaction record and allow the transaction record to used the process of registeration, confirmation, and sending the money. Now Blockchain technology is being used in different areas in our real world like in commercial transactions, healthcare, land & property holdings, and also somehow in the government sector [4].

The main field where blockchain is implementing, is attaching cryptocurrencies with present banking systems and commercial institutions which creates a ecosystem which is too innovative in the banking sector.Thats why by allowing blockchain into commercial/financial institutions to start their transactions without the support of any central authorities or third parties. Then each transaction must be secured and authenticated over more than half of network which are competing in the whole network of blockchain. Hence it means their is no any member who can be able to update or modify any data without the approvel of other members of the blockchain network.

OBJECTIVE

The objective of this paper is to analyze the awareness of blockchain technology and its present real world applications. Rest of the paper is defined by these sections.In section II their is some discription on the fundamental of blockchain technology, while in section III it describes the detail regarding the applications of blockchain in the real world. Section IV describes advantages and challenges of the blockchain.Finally at last few conclusion has been suggested in section V.

Section II

FUNDAMENTAL OF BLOCKCHAIN TECHNOLOGY

Block chain is a decentralized system of secure and trusted distributed databases (distributed ledger). Which record and share the transaction details across with many nodes which are the part of the network so that the data can’t be modified.[4].Nowadays, cryptocurrencies have appeared as outstanding package systems. Seeing here the mentioned Fig. 2, the primary block or we will say the genesis block that isn't appeared within the fig contains the first dealing. The hash function of the primary block is forwarded to the small block which is under the blockchain,then the minor block creates the hash function for second primary block. In similar manner, both two blocks creates a hash for the third primary block and this third block is the combination of these two blocks. All blocks within the blockchain may be derived back to the origin block [12]. For example, The hash algorithm or hash code for bitcoin is SHA-256,similarly Litecoin [5] and Primecoin [6] works on Scrypt and Cunningham chain/Bi-twin chain algorithm respectively. It also verifies the input mapping to the acquired hash code also it is not possible for having same hash for two different inputs [7]. In bolckchain the balance-sheet/ledger has validated and being taken care by node of network which are collection of rules ,through which it grants users to access and reach a common agreement thatswhy it doesn’t required a third party or any central power[8]. Every node keeps and saves a full clone of whole account/ledger.The main aim of the blockchain technology is to resolve the issues which are present in cryptocurrency like bitcoin or any other. In blockchain, the basic process of generating new blocks comes with the help of Mining Process. With the help of blockchain all nodes is to be verified whether the coin which we are using is valid or not, means whether the current coin is new or already in use if the coin is in use then their is no any need to create such coin that is not valid. Mining process is a process which requires important system resources,time,absolute access to a big amount of data, which makes it quite hard for a third person/attacker to make a transaction.The followings are the prevalent steps in cryptocurrency:

(1)A pbulic key is assigned to the user , is available for a user who has a wallet.

(2) In user wallet a private key is available which is useful for signing in the account transaction and also for proving dominion.

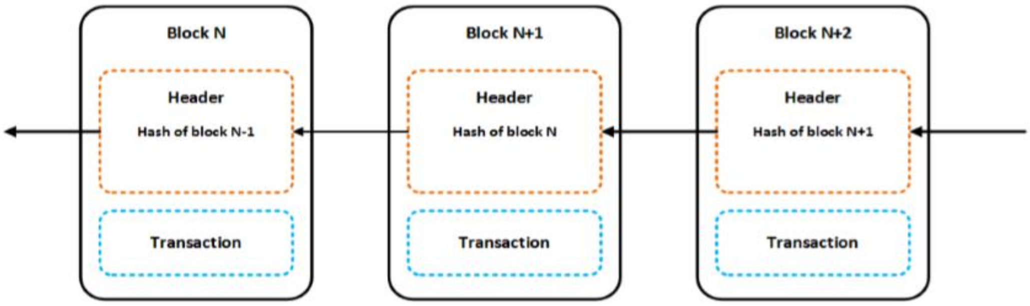
(3) The user who is paying the coin he/she sends coin to the acceptor by the blockchain address and then sign the transaction with the help of his/her private key then at last with the help of mining process the account/transaction is being validated.

Here are some cryptocurrencies are covered in our paper, (Table 1) reviews the existing cryptocurrency systems with its hash function and programing languages, which are presented in global world.

Cryptocurreny	Year	Founder	Hash Function	Programing language of implementation
Bitcoin	2009	Satoshi Nakamoto	SHA-256	C++
Litecoin	2011	Charlie Lee	Scrypt	C++
Peercoin	2012	Sunny King	SHA-256 d	C++
Primecoin	2013	Sunny King	Cunningham chain	TypeScript,C++
Ripple	2013	Chris Larsen &	EC digitalsignature	C++

		Jed McCaleb		
Ethereum	2015	Vitalik Buterin	Ethash	C++
Auroracoin	2014	Baldur Odinsson	Scrypt	C++
Dash	2014	Evan Duffield & Kyle Hagan	X11	C++
Namecoin	2011	Vincent Durham	SHA-256 d	C++

(Table.1)



(Fig-2)

Section III

REAL WORLD APPLICATIONS IN BLOCKCHAIN

With the help of this section, we are explaining the real world application of blockchain technology. However, thier are too many applications but here applications have been combined into few groups likecommercial/financial services, healthcare, Shipments industry.

1.Healthcare:- Health care suppliers will influence blockchain to firmly store their patients medical records.Once any medical history is formed and signed within the care organization, then it is recorded into the blockchain, that ensure the patients with the proof and confidence that the record can't be manipulated. These personal health reports can be encrypted and hold on on the blockchain with a non-public key,in order that they are not accessible by any third parties solely accessible by bound people to confirm privacy.However, managing care knowledge is not an easy task,significantly just in case of privacy problems. Care knowledge shouldn't be disclosed to different parties that it would be liable to be used venally by malicious users or attackers.In order to urge the higher of these issues, a health care data gateway (HDG) supported the blockchain storage platform is projected by Xiao Yue in his own paper.[9].It's a smartphone based application which might be accustomed manage and management the information sharing simply.The projected system permits users to take the patient knowledge while not exposing patient privacy. However, a non-public blockchain cloud is employed to hold on the information therefore making the medical data can't be altered by anybody, together with physicians and patients.

2.Commercial/Financial Services:- Now blockchain is generally used for money transferring or we can say money transaction in commercial or financial sector that is thus processed by cryptocurrency.Money establishments like banks solely operate throughout business hours, six days in an exceedingly week. which means if you are trying to deposit a check on weekday at three p.m., you'll wait till next operating day to test that money hit your account.Although if you create your deposit throughout business hours, the dealing will still take 1-3 days to verify if their is big volume of transactions that banks must settle. Blockchain technology, on the opposite hand, it ne'er sleeps.[10] By applying blockchain technology into banks, shoppers will see their transactions processed in as very little as ten minutes,so essentially the time it takes to feature a block into the blockchain is nearly some hours time. With the assistance of blockchain technology, banks even have the liberty to exchange funds between establishments additional quickly and firmly[10].

3.Shipments:- Blockchain technology are often utilized by the suppliers to put into action, by storing the records of the origins of materials that they need purchased.This is able to permit firms to verify the correctness of their product together with health issues and morality labels like Organic factor, native issue, and truthful Trade.Blockchain are often wont to store data regarding the cargo at notably every section together with the world issue, date and time live, cargo taking care of individual points of interest, temperature, state of the item, and so on. Through this it'll facilitate to test endlessly if the cargo has been taken care of and it's touched base on time at any given space. it'll likewise facilitate the retailers find the lost or injured things within the shipments.[11] Throughout the item review, a certain record of store network can change the retailers to acknowledge the supply of the problem, the things that are influenced, that contain the problems.

Section IV

ADVANTAGES OF BLOCKCHAIN

In this section, we are discussing the advantages of blockchain technology in different areas.

Accuracy:- The accounts/transactions which are occuring on the blockchain network are approved by a network of huge number of computers.So this prevents most human involvement within the verification method through this we have a tendency to acquire a additional correct record of data and a less human error. Whether or not a computer on the network were to create a machine mistake then that mistake would solely be created to at least one copy of the blockchain[10].

Cost:- Mostly, in banks if consumers wants to deposit amount then bank wants to verify the transaction and somehow a third person or witness to validate the document.But in blockchain it removes the use of third person verification and the costs which is associated to him/her.The current system for example if the person use the credit card then he/she have to give few charge to the banks for the process the transactions.[10]Besides this Bitcoin does not have a central power and it doesn’t takes virtually no transaction fees.

Decentralization:- Blockchain doesn’t work on centralized software architecture which suggests it doesn't store its data in central node.Rather then, the blockchain is derived and unfold its info across a network of computers. At any time once a brand new block is added each computer on the network of blockchain updates its blockchain blocks to replicate the amendment.In place of storing it in one central information,it shares that information across a network ,through this it becomes harder to tamper with the data. If a replica of the blockchain goes into the hands of a third person or hacker it will compromised with solely one copy of data, instead of the whole network.

Efficiency:- Nowadays transactions placed through a central authority will take up to some days to settle. If you try to deposit a check on Saturday evening, you will not see funds in your account till next operating day. Alhotugh banks and financial establishments operate throughout business hours and six days in a week. Whereas blockchain is functioning twenty four hours every day, seven days in every week. Here the transactions may be completed in concerning ten minutes and might be thought-about secure once in simply some hours. This can be chiefly helpful for all cross border business, that takes an excessive amount of longer time due to time zone problems and also the ensure payment process by all the parties.

Privacy:- The networks in blockchain work like a public databases, that means that anybody with a web affiliation will read an inventory of the network’s dealings history. Whether or not users will access their information regarding transactions, the system will not provide to access the knowledge regarding the person who is creating those transactions. It's a typical a wrong perception that blockchain networks like bitcoin are unknown, once after all they're solely confidential.When someone makes a public transactions, their distinctive code additionally known as as a public secret's code is saved or recorded on the blockchain, instead of their personal info. though a person’s identity remains connected to their blockchain address, this prevents hackers from getting a user’s personal info.

Security:- In blockchain when a transaction is being saved,the blockchain network verifies its credibility and authenticity. Many of computers which are related to blockchain verifies that the information of puchasing[10] is correct or not. Once substantiating the dealings by the pc, it's accessorial to the blockchain within the kind of a block. every block on the blockchain contains its own distinctive code or we will say it unique hash .Once the data on a block is altered in any manner then the block’s hash code changes but their is not any any hash code shown on the block. This distinction makes it very tough for info on the blockchain to be modified rapidly.

Transparency:- In blockchain the non-public data or we can say personal info is stored as private,in other word the blockchain is relatively open source. Which implies that persons which are connected on the network of blockchain will update the code as they see the large no of network's power power backing them. As blockchain technology relies on open source[10] which means the information which we are storing in it is also open source,through the transparency of open source it is quite hard to manipulate with the informations.It is also impossible to change anything in blockchain through anyone because their will be millions of systems attached with the netwok at particular time.

CHALLENGES

As thier are quite a big beneifts of the blockchain, there are some challenges to implement or accept this technology in the ground level. The obstruction of the blockchain technology is not technicial implementation but the main challenge are politics and regulatory froces in allover the world. And also to implement the large networks in blockchain and its software design and programing costs too much time and money.Blockchain technology is not so much popular yet but we can say it is rising slowely thats why their are very few frameworks are thier in the present time, thats why for some couple of years their is less amount of genuine dangers with blockchain may not be visible till it progresses becoming more standard and successful.As a basic general framework blockchain also could have some weak information. Their is no doubt that the cryptography and digital transactions are secure with the help of blockchain technology because they are implemented according to the best business rules.

Section V

CONCLUSION

In this paper we discuss the fundamental of blockchain and its related application with advantages and some challenges which are not backing this technology. The technology is not yet in a good level but in future with some good work on this field it will deal with a large sectors of the world and also the cryptocurrency produces a better base for blockchain technology in future.We can eaisly say it will convert the present ecosystem of any sectors into the new effective way.However we can say that the technology at present time still has some way to go at another level where it will be implemented in the sectors like banking,healthcare,real-state and others which are mentioned above.

REFERENCES

[1] A. S. Tanenbaum and M. Van Steen, Distributed systems: principles and paradigms. Prentice-Hall, 2007.

[2] D. Drescher, "Blockchain basics," Springer, Tech. Rep.

[3] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” URL: http://www.bitcoin.org/bitcoin.pdf, 2008.

[5] C. Lee, “Litecoin,” 2011.

[6] S. King, “Primecoin: Cryptocurrency with prime number proof-of-work,” July 7th, 2013.

[7] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography. CRC press, 1996.

[8] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain,” in Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on. IEEE, 2015, pp. 577–578.

[9] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,” Journal of medical systems, vol. 40, no. 10, p. 218, 2016.

[10]“Reviewed by Luke Fortney, Blockchain explained” ,URL:https://www.investopedia.com/terms/b/blockchain.asp

[11]Shiv Raj Sharma,“Blockchain Technology review and its scope” in 2017 International Research Journal of Engineering and Technology(IRJET)Volume: 04 Issue: 12 / Dec-2017

[12] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, “A brief survey of cryptocurrency systems,” in 2016 14th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2016,pp. 745–752.