National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Case Study on Block Chain for Current Era

V. Prushotam, Vibha. B. G, Dr. Kavitha

Department of Computer Applications, Dayananda Sagar College of Arts Science & commerce, Bangalore, Karnataka, India

ABSTRACT

In the current era blockchain is new technology used to record transaction between two parties. It is a public ledger in which everyone is able to have access without central authority having control. This technology is very much essential for the finance sector, banking sector, government sector. In our research we have focused on the applications of the block chain, what all are the major technology used in the bockchain and comparative study on the various technology used in blockchain. The blockchain technology is 30% used in banking and finance sector,13% for government and public goods,8% for media and music.

Keywords : Blockchain,

I. INTRODUCTION

Blockchain is the main technology for the digital cryptocurrency bitcoin. It is a distributed database which records all the transaction that has been done and shared among two parties. Each block in block chain contains a single transaction of amount between the two parties. Bitcoin is the most popular cryptocurrency an example is blockchain. The first existence of blockchain came in to when "a group of people named SantoshiNakamoto first time published about the bitcoin". This was the first time when blockchain came into existence. This technology is used to record all the transaction in the format of digital ledger which is distributed all over the world by the networks. We can record any transaction what we did for ex, from buying of assets till paying money to the seller. The most important use of blockchain is the bitcoin. It is a cryptocurrency which is used to do all the transaction online. In this paper we are going to study about what is block chain, what all are the places where blockchain is used, what all technology involved in the block chain, comparison of blockchain technology. At last we will summarise This paper and elaborate upon future trends in this research field.

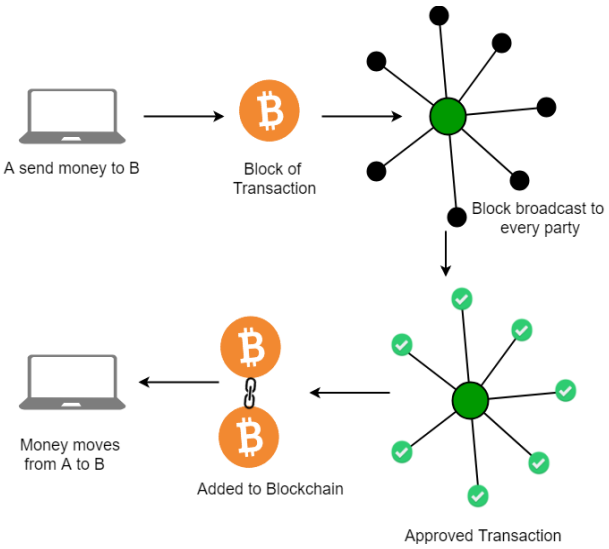

Fig 1.Blockchain Transaction

II. DEFINATION OF BLOCK CHAIN

A blockchain is a growing list of records that are increasing day by day. Every blockchain contains blocks. Each block contains a single transaction that is done by the two parties and it also contains a cryptographic hash of the previous block, and a timestamp. Once the transaction between the two

parties is recorded then it is difficult to alter. This is why blockchains are considered as secure design.

This blockchain was firstly invented by a group of people using the name of sasntoshinakamoto in 2008 to serve the public transaction through the use of cryptocurrencies (bit coin). This blockchain also solved the problem of double spending without the need of a trusted authority or central server.

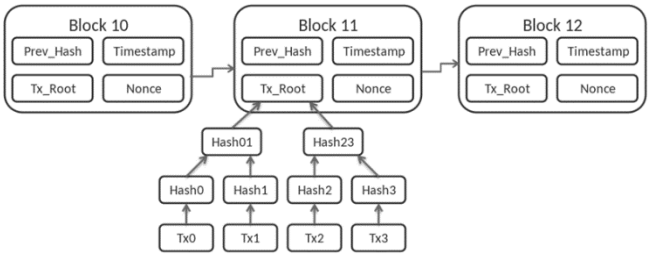

Fig 2. Blockchain diagram

III. MAJOR APPLICATION OF BLOCKCHAIN AND ITS USES

FINANCIAL SERVICES:

Block chain technology in finance:

In financial services blockchains can be used in an efficient way as there are transaction between two parties in the financial service. Financial sector activities ranges from backend clearing and settlement, to global capital markets architecture. So in this sector we can introduce digital ledgers system so that what all transaction done between the two parties are secure. This is how we can introduce blockchains in financial services.

Fig. 3. Blockchain Technology in finance

GOVERNEMENT:

In government sector also we can introduce block chain system which is Distributed Ledger Technology (DLT)). If we introduce this system in the government sector we can improve govt services and there will be faster communication between government and the citizen .this system is more efficient and secure for data sharing.

Fig.4. Blockchain technology in government

HEALTHCARE:

In healthcare sector we can introduce block chain system or we can just use Distributed Ledger Technology (DLT)) to record the patients transaction. Which patents are coming at what time and how much they are spending. We can record all these transaction through DLT ledger system. In now days we use pen paper to record the transaction instead we can use DLT ledger system so that the data is more secure and efficient.

INSURANCE:

In insurance sector we can use block chains to record the data between two parties. If we use block chain system then we can overcome from the problem of data sharing, data security which comes in recording the transaction through pen and paper. This is why nowadays many are changing to Distributed Ledger Technology (DLT).

Fig.5.Blockchain technology in healthcare

MONEY

In transferring of money between two parties the block chain technology is used. Block chains are more secure to use. And blockchains also provide a permanent record for the transaction that has been done between two parties. We cannot delete the transaction what is done. This system shows that how secure is the blockchain technology is. If we transfer the money through bank then there will be 3 parties involved in the transaction. This system involves peer to peer transaction means person to person. In this system only 2 parties are involved. This is why this technology is more secure and safe.

Fig.6.Blockchain technology in money

IV. BLOCKCHAIN ALGORITHM

Blockchain is growing rapidly and it is collections of records linked to the powerful cryptography. Cryptography has written code that will require which has authorized decoding and encryption. Cryptocurrency uses cryptography for security reasons and to record transaction using blockchain technology which is discussed further. Adding the collections of records for validation of transaction is completely referred to as a blockchain algorithm.

TYPES OF BLOCKCHAIN ALGORITHM

From the introduction of blockchain and bitcoin and cryptocurrency in 2009 by Satoshi Nakamoto, many other algorithms have been accepted. Several such algorithms are continuously developed which also has main aim for solving the errors in the already existing algorithms such has PoW. Both Proof of Work and Proof of Stake are both present in consensus algorithm. They all the nodes of blockchain to and prevent from double spending, it also prevents from an attack which always attempts to spend the same coin repeatedly.

CONSENSUS ALGORITHMS

The introduction to blockchain bought the acceptance of consensus algorithms; even several more algorithmshave been accepted. These algorithms are very complex but it assists when the coins are purchased or while a node is running. It achieves the constant growth which contains multiple nodes, and also it makes sure all nodes are proper to the said rule or action.

Nodes tell the consensus is a bitcoin, but not the minors. Consensus is always told as chain with most of the work. Nodes present in consensus accept the transactions, blocks with validations, blocks replication, block serving, last but not least storage of blockchain. Nodes also define PoW(Proof of Work) algorithms that has been employed by minors.

COMPARISON OF THE FIVE CONSENSUS ALGORITHMS

characteristics	consensus algorithms				
	PoW	*PoS*	*DPoS*	*PBFT*	*RAFT*
Byzantine fault tolerance	50%	50%	50%	33%	N/A
crash fault tolerance	50%	50%	50%	33%	50%
verification speed	>100s	<100s	<100s	<10s	<10s
throughput(TPS)	<100	<1000	<1000	<2000	>10k
scalability	strong	strong	strong	weak	weak

Fig.8.Comparison of five consensus algorithms

MINING ALGORITHM

In mining algorithm the data mining has three main components they are

- Clustering or Classification
- Association rules
- Sequence analysis
- Clustering or Classification: It is examination of a group of data and also to generate a group of grouping rules which is used to keep the order of future data.
- Association Rules: It is a rule which has a specific alliance relationship between the group of objects in database.
- Sequence Analysis: It is the complete analysis of patterns that will come in sequence.

There are many more of such algorithms which has given the ides to implement like those aspects in data mining.

In blockchain, the data miners use their computer to repeatedly and also to guess the answers to the puzzle among a group until one of them in the group wins. More importantly the data miners use the blocks unique header metadata using a hash function in it which will also return a secure length of random string numbers, it uses the hash value to modify the nonce value in the data.

If a miner recognizes the hash functions that has the similarities of that of the target then the miner will be rewarded in cryptocurrency and also the blocks will be emitted across the networks for each of the nodes to also validate and add their own ledger copy. If miner B finds the hash before minor A, minor A will stop its process and process the remaining blocks.

V. TRACEBILITY CHAIN ALGORITMS

Traceability demonstrates the origin & practices the transaction when it is collecting extra information to improve the internal performance process and activity of each node in the supply chain. The major aim in traceability chain algorithms is to grab the decisions quickly and in speed. Accordingly, such as operation which produces the irrelevant information problems and it also optimizes the traceability in blockchain poorly. The AI(artificial intelligence) of a mining blockchain algorithm, it runs more faster than consensus algorithms because of inference mechanism.

Nowadays the companies are not able to trace items repeatedly because of data in silos which is corresponding with repetitive points. Using block chain we can repeatedly trace the journey of the transactions. A new approach called Takagi Sugeno Fuzzy cognitive maps applies this traceability chain algorithm. Biased functions for optimized decision compute are described as the participant node constraint method. Thus definition succeeds in meeting the less mining efforts when the traceability chain is process in done.

To grow a fully traceability system, there should be motion of a transactions on the blockchain, giving the each item that will link to the transactions a virtual identity. For that objects have to be linked with all sensors that will store data about items and transfers them to a particular platform. For ex: QR codes, RFID, or wireless sensor networks. A traceability algorithm consists of three main sub-processes:

1. Identifying and naming of products to facilitate the product name.

2. Data capturing and recording: Scans the capacity with electronic data flow to optimise retrieval of information.
3. Linkage & communication is needed to optimize the information sharing which happens between supply chain partners and protocols.

The cooperation between the traditional traceability tools and blockchain guarantees monitoring of transaction without any interruptions the supply chain acts as a major shield against markets performing poorly.

VI. WHAT ALL TECHNOLOGIES USED IN THE BLOCK CHAIN

The basic and most important technologies used in blockchain are:

- Decentralisation
- Tranparency
- Immutability

DECENTRAILISATION:

Earlier centrailized services were more used commonly used. But in now days tradition hass changed a lot. With the brought up of the new technology bitcoins and the bittorrents technology has changed a lot. Earlier in centralised system we used to depend a lot on a particular entity for example earlier if we want to send money to someone we used to depend on t he entity named bank if we want to transfer money . If bank is not there then we cant do the transaction part in the centralised system. But in these days trend has changed .bit coins and bit torrents are the example of the decentralised system. In decentralised system what we do is that we don't depend on any type of entity so the transaction is in the very easy manner.

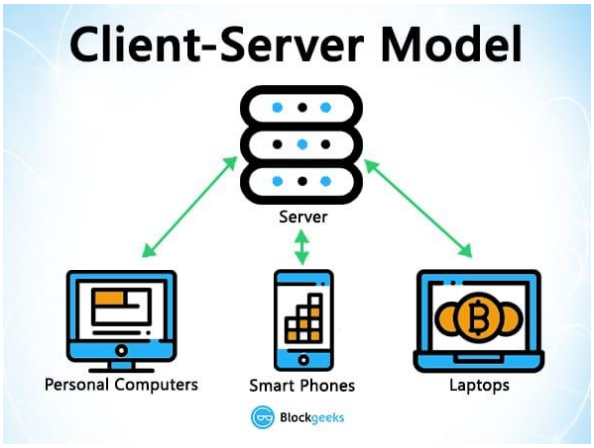

Fig.9.Client-Server Model

TRANSPERECY:

In blockchain the most important and misunderstood concept is its transparency. Most of the people think that transparency means hidden or privacy from the public or transparent…? What do you think so?

So lets understand the concept of the tranperency in the blockchain . In blockchain with the help of transperecy technology we can hide certain information from the public while doing the transaction it will not show the name of the person instead it will show the public address . foreg "Bob sent 1 BTC" instead you will see "1MF1bhsFLkBzzz9vpFYEmvwT2TbyCt7NZJ sent 1 BTC".

In blcokchain with the help of the transperecy technology people cant do fraud while doing the transaction. If we give the public address in the internet then it will show the full transaction that has been done by the party. For eg if there is a company and customers buy clothes from the compay for egflipkart if flipkart starts using this technology then the company can't do fraud in these. we can catch the company if company does fraud transaction.

This way we can maintain proper transaction records.

Fig.10.Transaction record

IMMUTABILITY:

This is the very most and valuable cocept used in the blockchain system. This technology is used in the digital transaction that are done by the 2 persons. In these the transaction that are entered once cant be changed this is the main feature of this technology . So if we start using this technology then we don't have to fiddle around with the company accounts and there will be no misuse of the transaction record details that are: deleting some of the transaction earlier people used to do it.

This technology uses a cryptographic hash function or hashing algorithm know as SHA-256.

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Fig.11.Cryptography

VII. COMPARISION OF TECHNOLOGY USED IN BLOCKCHAIN

BITCOIN:

This was the first and the earliest product of the block chain which used the system of decentralisation in the transactions that were done between 2 people. Bitcoin is a public type blockchain where anyone in invited to join. The main components that are used in the bitcoin mechanism are as follows cryptographic hash function, digital signature, private-and-public key encryption, peer-to-peer (P2P) network, and proof of work (POW) consensus algorithm.

This technology allows people to do non reversible transactions without having the use of the third party. A single transaction contains a unique transaction ID, input bitcoin address, the number of bitcoins to be transferred and the output bitcoin address of the recipient. In this technology every node has the complete information about the blockchain so this makes this decentralised one .

ETEHEREUM

Ethereum is different from bitcoin; it is built for allowing the transactions of crypto payment on a decentralized network. Ethereum was designed which has much larger aim in their mind. The developers can launch their own block chain projects which include their own cryptocurrencies the platform has been provided. The platform which is used to launch their projects commonly is called as Ethereum Virtual Machine (EVM) which has been used to launch over thousands and thousands of DApps. Using EVM many famous cryptocurrency projects which is VeChain and OmiseGo has been launched. Smart contracts like this make it possible.

These are the pieces of code, which will allow the execution of legal function such as taking control of an entity based on particular conditions, and based on fulfilling the required conditions the transferring crypto token is done.Ethereum proprietary language Solidity uses smart contracts on the Ethereum platform, which is motivated by C++ language, Java, Python and JavaScript languages. It also gives access to a way for the user to tell how much of computing power can be extended for a transaction, which uses to measure the processing power which is also called 'Gas'. The gas limit is specified by the user. The execution of a transaction is done which remains within a limit, like wise, the changes are made when it exceeds the limit. The requirement of the gas is less when it is simple payment transaction, if it is more complex operations for ex: deployment of smart contracts requires more gas.

RIPPLE PROTOCOL

It uses most of the features of Bitcoin/Ethereum which is decentralized design and cryptographic hash functions and P2P network, and private public key encryption. The Ripple Protocol was specifically designed to facilitate rapidly and less of global transfer of money, which gives so many unique features in each one.

RPCA happens in 5 rounds and they are:

- At first each server takes all valid and also unapplied transactions and makes a list, public in the form of a candidate set.
- Each and every server has one unique node list (UNL), where the other entire server queried by this server is listed.
- Each and every server takes all candidate sets of entire servers in its unique node list and together makes a mixed list, before voting on the unique node list.
- Transactions thathave been received larger than the threshold of 'yes' votes then it is taken to next round, and the others votes are discarded/moved to the candidate list for next round.
- The final round always requires an average of 80% of the servers on a server's unique node list to be considered on the transaction and before being applied to the ledger.

  After applying to the ledger all the accepted transactions in the ledger, the ledger is will be closed, and it is named as new last closed ledger.

VIII. CONCLUSION

Hence we conclude that it is very useful to understand the concept of the blockchain in these days. Earlier people used to think that all blockchain mechanisms uses the bitcoin technology but it is not true. These days many new technology came which uses the system of Blockchain like pow, longest chain rule,etc. bitcoins were the first to maintain decentralised, public ledger with no formal control or government. These blockchain system will now solve the problem of pen paper ledgers which were earlier used. This technology also has lots of pros and cons.

IX. REFERENCES

[1]. Introduction-https://www.google.com/amp/s/www.geeksforgeeks.org/blockchain-technology-introduction/amp/
[2]. definition of block chain:https://en.m.wikipedia.org/wiki/Blockchain
[3]. major application of block and its use:https://www.blockchaintechnologies.com/applications/
[4]. blockchain algorithms: https://blog.goodaudience.com/a-simple-introduction-to-blockchain-algorithms-ca05b9bcc32f
[5]. what all technologies used in the blockchain:https://blockgeeks.com/guides/what-is-blockchain-technology/
[6]. comparision of technologies used in blockchain:https://medium.com/edchain/a-comparison-between-5-major-blockchain-protocolsb8a6a46f8b1f

Cite this article as :

V. Prushotam, Vibha. B. G, Dr. Kavitha, "Case Study on Block Chain for Current Era", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 55-61, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194710