BLOCKCHAIN: WORKING SYSTEM, CONCERNS AND IT'S FUTURE

Kamalesh V R A,
B.Sc (Computer Science),
Department of computer science,
Sri Krishna Adithya College of Arts and Science,
Coimbatore, Tamil Nadu, India

Amrutha S,
B.Sc (Computer Science),
Department of computer science,
Sri Krishna Adithya College of Arts and Science,
Coimbatore-641042, Tamil Nadu, India

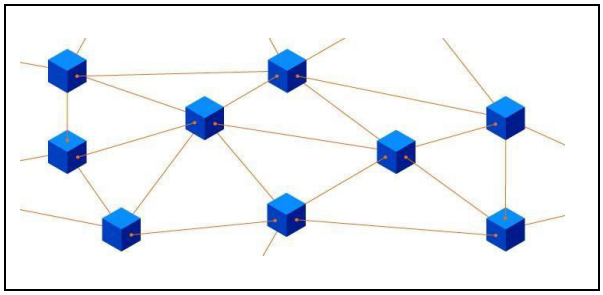
Bhuvaneswary B,
B.Sc (Computer Science)
Department of computer science,
Sri Krishna Adithya College of Arts and Science,
Coimbatore-641042, Tamil Nadu, India

ABSTRACT: Now a day's blockchain has received the great attention from all the multi-national companies.It can be considered as advanced technology that brings more benefits to many different sectors. It is recently updated technology and it revolutionizes the whole digital world which brings new things such as security and efficiency. The main objective of this concept establishes a system that creates a distributed unity in the digital online world. This allows everyone to know about the digital event which is happened by creating a record in the public ledger. In the future, it provides very low-cost trading's with trusted peoples. This white paper describes this technology concerns, challenges ahead and the opportunities in the digital online world.

Keyword: *Blockchain, distributed ledger, bitcoin*

I. INTRODUCTION:

A blockchain is a distributed ledger or database of records or public ledger of transactions of the digital event which is maintained by the network nodes. The blockchain is public and once entered, information can never be erased or modified. This technology is a decentralized system which does not require any third party like as the organization in the middle. In addition, the nodes in the blockchain are unnamed, which makes more secure in between the transactions. Bitcoin is the first application which introduces this blockchain technology. This application creates a decentralized environment for the cryptocurrencies and it makes buy and exchange the digital money from the goods.



However, this technology is contentious and has worked without mistakes over the year and it being successfully applied in both finance and nonfinancial applications. The distributed technology model is the most important invention since the internet itself.

This is not a limited to the financial application, instead, it gives a great attention for every platforms or product to require the trustees. This technology has a potential to improve the systems throughout the society. In this technology, the idea is able to establish and verify the trust without using the centralized manner. It can perform fully based on the decentralization.

II. BACKGROUND:

This is a core technology which is used to create cryptocurrencies and bitcoin for the immutable distributed ledger. This technology was proposed by Satoshi Nakamoto in 2008. During the initial stage, this technology was not able to get a lot of attention. However, the bitcoin runs safely through this years. Nowadays, this technology is the hot topic in more countries, institutions, and researchers. This system can be applied in many fields like financial areas (cryptocurrencies), ethereum and zero cash.

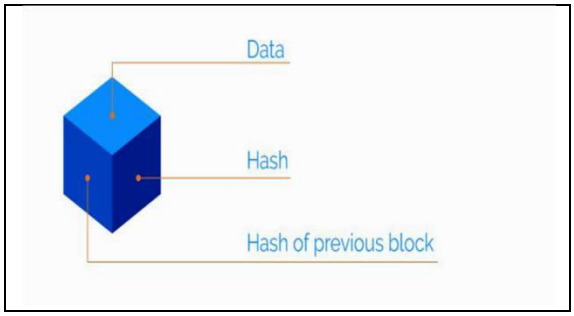
For example, bitcoin is the first transaction system which runs under the bases of the peer-to-peer network in the blockchain technology. It can adopt hash based Proof-of-work in the distributed consensus algorithms.

III. HOW BLOCKCHAIN WORKS:

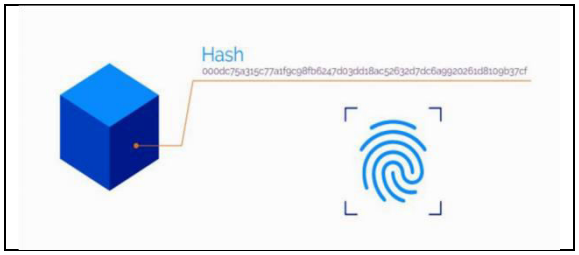
The blockchain is a very spicy topic around the world nowadays. The first blockchain was introduced in the research scenario in the year of 2008 for the bitcoin initiative. The main thing in this concept is transferring money from one tone without the intermediates.

The blockchain is a chain of blocks which is ordered in the network for the non-trusted peers. Each block has a reference about the previous one and that contains data's, hash value and the hash of the previous block.

BLOCK: The set of data stored inside a block which represented by any values and depending on the type of the blockchain. The single block can store the amount of money or a share of the company or a digital certificate or any other value. A block also stores the detail about the sender and receiver identifiers.



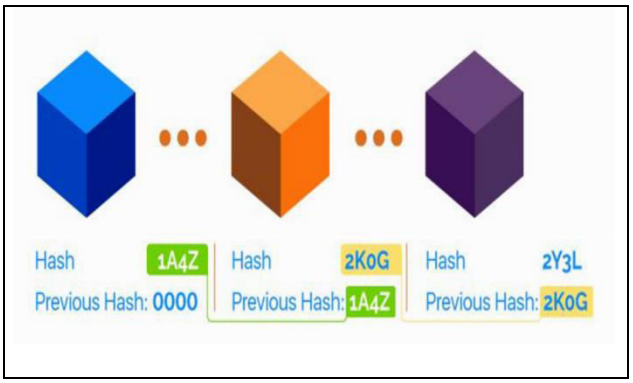
HASH: Each block has a hash. This value has been generated from the string of texts by using the mathematical function.



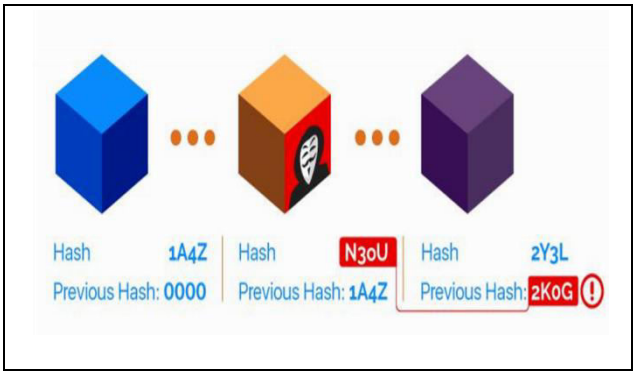
This value can be compared to our fingerprint, and every single hash value is unique. Once a block is created, a hash value is calculated within 10 minutes

HASH OF PREVIOUS BLOCK: A block contains the hash of the previous block.

For example, there are three blocks are created, the block 3 hash value is associated with the block 2 and block 2 is associated with the block 1 and the block is special, it doesn't point any block and it can be called as genesis block.

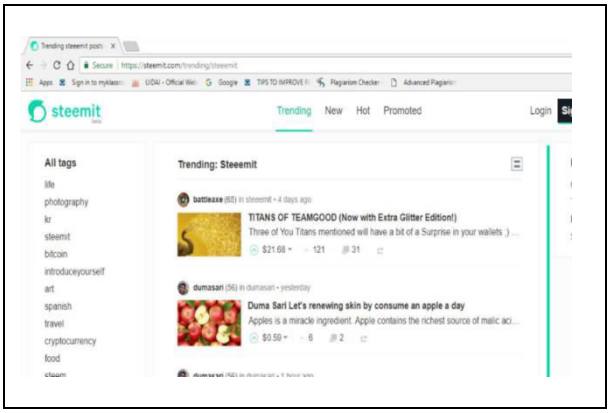


If anyone changes the value in the block that hash of the previous block changes, but it also makes all blocks as invalid.



The blockchain terminology also uses a process called as proof of work. This mechanism can participate in the network of the nodes which performs the work.

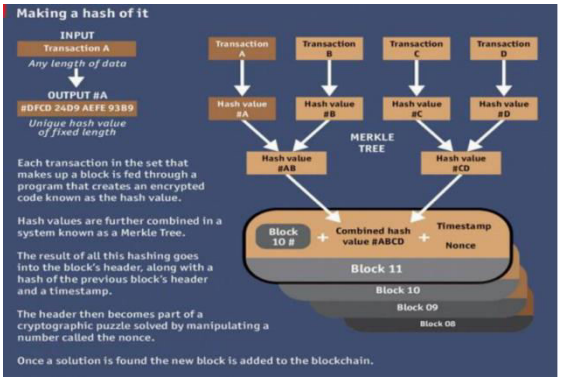
STEEMIT: This is the social news community network that works on the blockchain based platform for the publishers.



In this website, the user can launch our posts and comments similar to the other blogging websites or the social news websites like Facebook, Reddit. The users can receive the monetary reward as US dollars. It works in the decentralized platform.

IV. BLOCKCHAIN - DISRUPTIVE TECHNOLOGY:

1. Decentralized: The validation of every transaction must be performed by the network nodes without the need of the intermediations.
2. Data Redundancy: It can prevent the data's with the help of every network node and each node has a local copy of the blockchain.
3. Data immutability: The stored data in the blockchain could not modify or delete.
4. Transparency: This technology could act as a transparency which means everyone should read and the transaction stored in it.

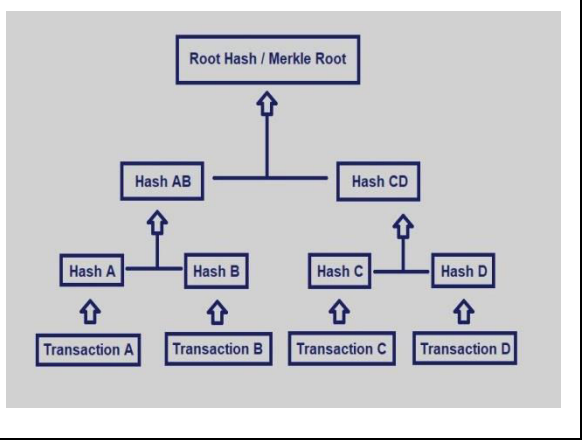


V. MERKLE TREE:

In this blockchain technology,the merkle tree is the heart of the blockchain technology.

It is a structure that can be an efficient and the verification should be secure. This tree can be used both the bitcoin and the Ethereum.

WORKING SYSTEM: It can produce all the transactions in a particular block by producing the fingerprint in digital form. It can be created repeatedly for the hashing pair, and it can be constructed from the bottom up known as transaction Id's.



Above example represents the set of blocks A, B, C, D. The hash can be stored in the leaf node. Hash A and hash B resulting as hash AB and the hash of C and D resulting as hash CD.

VI. BLOCKCHAIN TYPES:

The blockchain can be classified into three types, they are public, permission and private.

PUBLIC: In this blockchain, anyone can read and write on this platform.

PERMISSIONED: It can be a transparency where only selected persons can access the transaction. Read permissions can be restricted in this type.

PRIVATE: it can create a closed-loop environment. Write permissions are centralized and read to all participants.

VII. BLOCKCHAIN USE CASES:

- **Public blockchain: Bitcoins -** It is the most popular use case in the blockchain technology for the digital currency in a decentralized manner. Bitcoins are blockchain network by using the computing power to solve the mathematical puzzles. This software is open source so anyone can join to buy things electronically.
- **Permission blockchain:** Trade Finance Application. It is used to trade finance instruments for the manual purpose, it can be considered as the paper-based process.
- **Private Blockchain:** Loyalty Application In this system, high lag service and the credits can be the form of loyalty points, customers cannot use the checkpoints.

VIII. SECURITY AND SCALABILITY:

Giving a large amount of faith to this open source technology should provide assumptions under this circumstances. So, it can be considered as potential consequences before adopting this blockchain solution to store our every transaction, assets, and ownership's proof or the private information's. This network uses under the one way hash function, it is also a mathematical function that takes input strings and converts into a binary sequence. The newly generated blocks are in the form of the linear sequence of time.

EFFICIENCY: The data's which is stored in a block can be run automatically through the presented procedures. It can reduce the cost of labor but improves their efficiency.

IMMUTABILITY: Once the data can be stored in the blockchain no one can edit, not even a system admin, can change it. This system provides the benefit of an audit, and these benefits are more useful to the database of the financial transactions. In this technology, this system can be considered expensive. This system can work under the base of unchangeable.

SCALABILITY: The transactions on a blockchain have been imitational which is compared to the traditional financial network. It can support more than

ten thousands of transactions per second in the blockchain infrastructure. Every recordable transaction should require into the peer-to-peer verification. It becomes time-consuming with the involved set of blocks.

MALWARE: The blockchain can be used both the good and evil.

IX. IN EDUCATION:

Nowadays many of the institutions have applied this blockchain technology into the educational system and most of them to support the academic degree management.

This technology can compose the whole transcript. This educational system can be applied in many innovative ways just as diploma management and the achievement assessments. It has a great potential for border application that can formulate the evaluation, learning, design, and activities. In many of the institutions, most of the students are still negative subjective for the poor learning outcomes (financial pressure and the lack of motivation). By using the blockchain system that can motivate every student by implementing "learning is learning". Overall the blockchain technology should construct the balance to measure the learning process and final outcomes. And it is more reliable to every student.

X. BLOCKCHAIN TESTING:

Nowadays there are many of the blockchains should appear and more than 700 cryptocurrencies are developed. However, some of the developers should perform the blockchain to attract the investors to drive the huge profit. When the users want to coincide with the blockchain into the business administration, with the help of the requirements. So the blockchain testing needs to place the test in different forms. In this technology the testing can be classified into two phases, they are Standardization and the Testing phase.

By the STANDARDIZATION phase, the blockchain should be initiated it could be tested with the agreed criteria and the TESTING phase, It can perform different criteria.

XI. BIG DATA ANALYTICS IN BLOCKCHAIN:

The blockchain technology is combined with the big data. It can be categorized into combination into two types, they are DATA MANAGEMENT and DATA ANALYTICS. DATA MANAGEMENT, the blockchain should store the data in the way of distributed and secure. It also ensures the data into the original method. DATA ANALYTICS, the transaction must be used for the big data analytics.

XII. ADVANTAGES OF BLOCKCHAIN TECHNOLOGY:

In this blockchain technology, there are some advantages which are used in this application, there are,

The biggest advantage of this technology is disintermediation, it can enable a database should be shared directly without a central administrator. Blockchain can be acting as consensus to ensure the nodes, it can be sync and transaction can be verified and processed independently. Why is disintermediation good for us?

Because the database is the tangible thing in the form of bits or bytes. In the database, the content is stored in the memory disk in a separate computer system that can be run by the third parties like trusted banks and governments. Thus, the third party association can control the important database which is needed to hire many peoples an\d design many peoples who are all tampered with it. However, the blockchain can replace the third parties in the database. It can be increasing the computer's capacity to provide a new way that is replacing humans with codes.

PEER-TO-PEER GLOBAL TRANSACTION:

The blockchain technology fully works under the peer-to-peer payment services with the specific limitations such as location, restrictions and the minimum transfer accounts.

Other advantages are:

1. The users can control the transactions and information.
2. The data are fully complete, timely, accurate and consistent are available.
3. Due to the decentralized network, it does not have a central point of failure and the malicious attack.
4. All users can trust their transactions by removing the need for trusted third parties.
5. Once the data are stored in the block, it cannot be altered or deleted.
6. Transactions are added been single public ledger and it reduces the multiple public ledgers.
7. It helps to be the faster transaction of 24/7.
8. It reduces the transaction fees.

XIII. DISADVANTAGES:

The disadvantage of the blockchain technology is a performance which is slower than the centralized database. The transaction is being processed, it conducts an additional burden as well:

SIGNATURE VERIFICATION: The every blockchain transaction must have the digitalized signature by using the public edger.

CONSENSUS MECHANISM: It involves back and forth communication or dealing with the forks and consequent rollbacks.

REDUNDANCY: It can be a total amount of the consumption. It takes the lot of work is being at the same end of the result.

XIV. RESERVE BANK OF INDIA ACTIVITIES:

The RBI (Reserve Bank of India) has monitored the developments that can be related to the blockchain technology. In the year July 2016, IDBRT (Institute for Development and Research in Banking Technology) it can explore the applicable blockchain to the Indian banking and financial system to conduct the workshop for the stakeholders.

The most working group experts in the central bank, CCIL, ISI, TCS, Infosys, and Deloitte. These participants can work together to get output with the white paper dealing technology, global experience that can adopt the financial sector in India.

The white paper technology highlights the several advantages of using the blockchain technology. It can take part of cost savings, efficiency, and the transparency systems.

The IDRBT also can develop the proof of concept; it can apply for the blockchain to the trade finance applications.

XV. FUTURE USE CASES OF BLOCKCHAIN:

1. DAO:

DECENTRALIZED AUTONOMOUS ORGANIZATION, it is one of the functionality that can be supported by the Ethereum and it is essentially like an organization that runs under the some of the rules encoded by the computer systems.

It can be called as smart contracts. These small contracts are the software-based transaction that can be negotiated, verify and execute the systems automatically.

This system can be accessed by the group of peoples without leaders in the form of digital.

2. IoT:

INTERNET OF THINGS, it is nothing but the things can be connected to other things through the internet. In the blockchain, the IoT works with the centralized manner. In nowadays many of the devices grown up rapidly, by generating the transactions and the computational requirements. Blockchain technology will create the secure mesh networks.

Every single node can be connected with the blockchain, those devices can be identified and authenticate each other without the help of the humans. However, the device identification and the intercommunication are secured by the permission less blockchain that holds the node of the network by the use of unique identity.

3. SCM:

SUPPLY CHAIN MANAGEMENT, this is also a technology which is combined with the blockchain technology. These are one of the types of the network that can exist many of the stages and the geographical locations. Blockchain technology enhances the transparency method and security in the supply chain management. The change in SCM will lead to dynamic chains in the phase of accountability. These supply chains are regulated by the some of the companies in the distributed large scale system.

4. SPORTS:

This technology is also used in the sports as well. By the DCM, the smart contracts can be used by the traditional contracts between the sports player and the associated clubs. The tickets for seats in the stadium can be set into the public blockchain.

5. ARTIFICIAL INTELLIGENCE:

The combination of artificial intelligence, 5G, IoT and the blockchain should provide the ability to extract the intelligence; it can be starting from the global ecosystem that can always be connected with the sensors.

Many of the companies are working with this technology could be used for the purpose of the real-time tracking or reducing the waste and the costs.

In addition, the AI and the blockchain creates a solution to the worldwide distributed assets and record the management system.

6. GENECOINS:

These coins are the bioeconomy currencies. By the by Google discovers the new websites, it will able to jumps from chain to chain. Our important aim is to turn Genecoin into a DAO that preserves the genetic material.

XVI. CONCLUSION:

Gradually the blockchain technology is the most used and high impact application. It transforming the traditional industry with the method of decentralization, auditability. The goal of the blockchain to provide the security, privacy and the transparency to all the users. In this paper, we present a comprehension about the working system, concerns and the future of the blockchain. We first give how the blockchain works? Including the architecture and the social website with the disruptive technology. Then we discuss the types and the use cases of the blockchain. We discuss analyzed and compared the use cases and the testing with the blockchain. Furthermore, we listed some of the pros and cons of the blockchain technology. Nowadays blockchain-based applications are rising up and we plan to conduct in-depth researches on blockchain based application in the future.

REFERENCES:

1. "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1-2016/ [2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
2. G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," 2015.
3. K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, Germany, 2016, pp. 305–320
4. Holden J., The Mathematics of Secrets, Princeton University Press, (2017)
5. Kariappa, B. 2015. "Block Chain 2.0: The Renaissance of Money". Wired. Accessed 27 October 2017
6. https://www.wired.com/insights/2015/01/block-chain-2-0/.
7. Kashyap, M., Davies, S., Shipman, J. Nicolacakis, D. & Garfinkel H. 2017. PwC Global Fintech Report.
8. PricewaterhouseCoopers GmbH. Accessed 17 November 2017
9. https://www.pwc.com/gx/en/industries/fi nancial-services/assets/pwc-globalfintech-report-2017.pdf.
10. Kehril, J. 2016. Blockchain Explained. Niceideas.ch. Accessed 2 November 2017
11. https://www.niceideas.ch/blockchain_explained.pdf.
12. Future generation computer systems, Elseiver(IF:3.997)(special issue on blockchain and decentralization for internet of things
13. http://www.journals.Elseiver.com/futuregeneration-computer-systems/call-forpapers/special-issue-on-blockchain-anddecentralization-for-interne).