Blockchain Technology

Vijeth M S[1], Dr. Manjunath M[2]
Department of MCA
RV College of Engineering
Bengaluru -560059

Abstract
Blockchain is a latest technology, which has enormous application in variety of industries. It is mainly popular as an underlying technology for Bitcoin and many other cryptocurrencies. It provides new solution to the age-old human problem of trust, fundamentally Changing the way Internet transactions are implemented by detecting trust between unknown parties. In addition, they ensure irreversibility (once information is Has been entered, it cannot be amended), include arbitration (as assured of trust, no third party is required to verify the transaction) and the result is low cost (low fees.) These advantages and other disruptive changes can arise, When properly used. large number of applications are motivated to develop And implemented. These applications form the backbone of what can be called Internet of value is bound to bring about significant changes during The last twenty years by the traditional Internet. Nevertheless, we are still in the beginning To fully understand its potential, impact, challenges and possible future directions. This study uses the techniques behind it and the implementation areas and potential impacts.

Keywords: *Blockchain, Cryptocurrency, Ledger.*

I. INTRODUCTION

The Blockchain technology has been popular in recent years due to its decentralized, peer-to-peer transactions and immutable qualities. It is a digital ledger that is publicly available to all users in the network. It is derived from concept of Santoshi Nakamoto's 2008 bitcoin cryptocurrency. Since then, more than 2000 cryptocurrencies have been available in market. Although the use of bitcoin is still not widely available worldwide, Separate issues like money laundering, legal and illegal mining demonstrations are associated with bitcoin. Bitcoin system's mining process And verification of transaction takes about 7-8 minutes. This concept is useful for many application areas such as healthcare, Internet of Things (IoT), industry, supply chain management-etc. To analyze the technical implementation of blockchain, the main focus has been given to some recent developments by various organizations along with the application area from an academic point of view.

Blockchain technology transactions are publicly available to read but once recorded no one can modify the transaction. Extensive literature survey has been done and it has been found that blockchain is being used in many useful applications easy. Developers specify that the blockchain is a probabilistic state machine and is not useful where the finality of decisions is required. Developers explain some of the possible range of blockchain utility and explain how blockchain technology can be Different traditional databases are used in the problem. Currently blockchain technology is one of the most in-demand research areas, but it lacks technical details. It can be actually implemented in almost every field.

Many people think that blockchain is just a technology that empowers Bitcoin. While this was its original purpose, the blockchain is Able to do so much more. Despite the sound of the word, blockchain is not just one Single technology, it is an acronym of a suite of distributed laser technologies that can Anything of value can be programmed to record and track. It can be used for all types of assets, financial transactions, Medical records, utilities or even land and property registers. So it is decentralized system for everything of value. What makes things different here with blockchain, which is contrary to the centuries-old ledger system, Basically a book, then database files stored in a single system. Blockchain is decentralized, distributed across a large number of computers. This decentralization of information reduces the ability for data tampering, this brings us to another factor that makes blockchain unique. Second, the blockchain instills confidence in the data, before a new block is added to the chain, a few things have to happen. First, a cryptographic puzzle must be solved that is building blocks. Second, the puzzle-solving computer shares the solution with all other computers in the network. Third, network computers will then verify the solution, and if true the blocks will be added in series. This is called proof of work. The combination of these verification and math puzzles by multiple computers ensures that we can rely on each block of the chain. Because the network builds trust for us and we now have the ability to directly interact with our data in real time.

II. BLOCKCHAIN ARCHITECTURE

Blockchain is the technology behind bitcoin. It is a public distributed database that holds encrypted ledgers. Blockchain is a technology in a global database that anyone, anywhere, can use with an Internet connection. Unlike a traditional database, which is owned by a central party like banks and governments, a blockchain belongs to no one. Together It makes it almost impossible to spoof the system by providing a complete network that takes care of it, fake documents, transactions and other information. Blockchain permanently stores information between nodes in a network. It's not just decentralization Information but also distributes it. Each node in the network can store a local copy of the blockchain system. It is periodically updated to keep uniformity between all nodes. A blockchain is a distributed computation and information A sharing platform that enables multiple nodes that do not trust each other can take the decision-making process. Problem There is a single point of failure in a centralized system. A decentralized system has many coordinate points that are over-Come single point of failure. Each node in a distributed environment collectively performs tasks. The picture above shows the basic Architecture of Blockchain. Each user is represented as a node connected in a distributed manner. Each node retained a copy of Blockchain list that is regularly updated. A node can perform various activities such as initiating transactions, verifying a Transacting or mining.

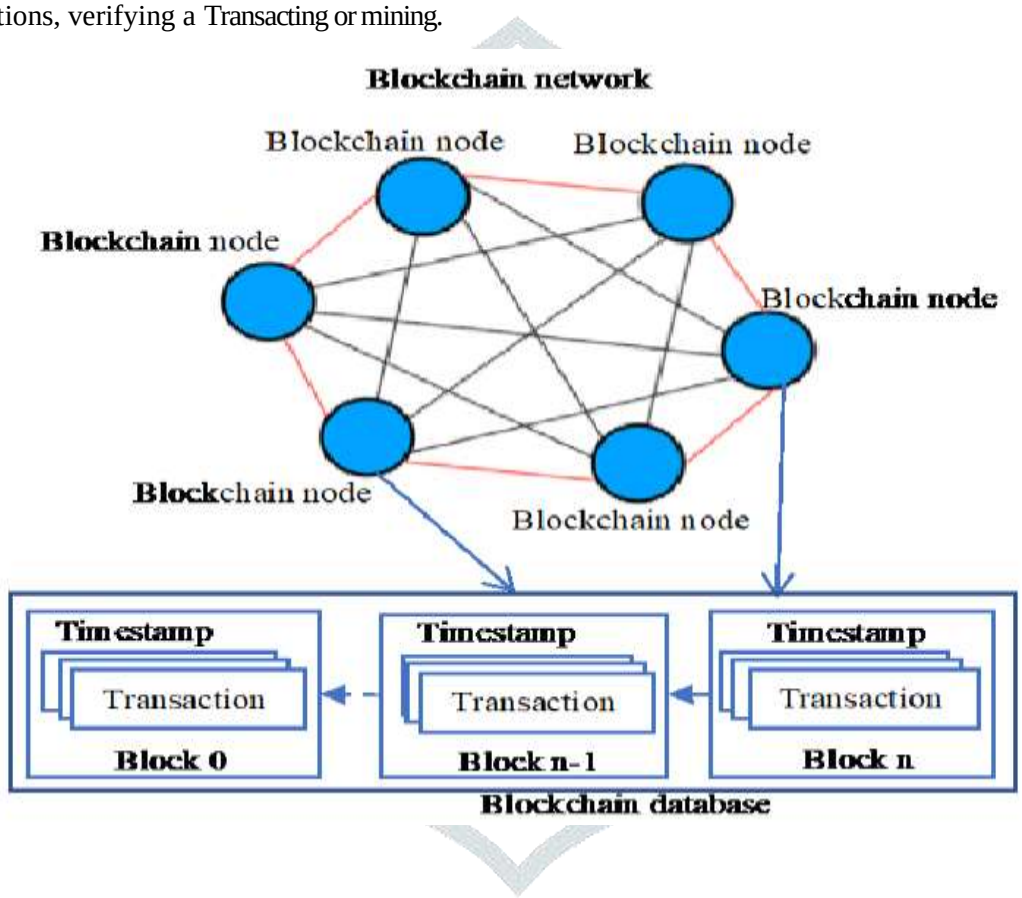

Fig 1: Architectural Diagram

III. STRUCTURE OF BLOCKCHAIN

- Block:

In blockchain, a block is a collection of valid transactions. Any node in a blockchain system can initiate transactions and broadcast to all nodes present in the network. Network nodes validate transactions once using old transactions the transaction is valid. The next step is added to the existing blockchain. How many transactions occurred in relation to? That time frame is grouped as part of the block and then stored in the blockchain block. "There may be a block" in bitcoin There are more than 500 transactions on average, the average size of a block is around 1 MB (an upper limit proposed by Satoshi Nakamoto in 2010) . It can grow up to 8 MB or more (as of March 2018). Larger blocks can help in Processing a large number of transactions at once.

- Block header:

Block header consists of metadata about the block.

- Previous block hash:

Each block inherits from previous block. The system here uses previous block hashes to create new block hash

- mining statistics:

This mechanism should be complicated enough to make the blockchain system tamper proof.

- Merkle tree root:

The transactions in the blockchain are organized in this merkle tree structure. The root is verification of all transaction. The toughness of the blockchain is determined with the difficulty of mining algorithm.

IV. TYPES OF BLOCKCHAIN

There are different design options (or models) for the blockchain. These options are based on who should be allowed to participate, inspect the data in the blockchain Network. There are basically three types of blockchains based on it: private blockchain, Consortium blockchain (group of organizations sharing common interests or concerns) And public blockchain. Whereas, we believe that consortium blockchain is a type Of private blockchain. However, the consortium blockchain is broad in scope. Group some areas together under a single blockchain network. Those types are sometimes regrouped based on the perspective of permission. They are divided into three categories: open blockchain for open access, closed blockchain for restricted Access and Hybrid Blockchain falls between the former types for customized access.

- Public:

It has ledgers visible to anyone on the internet and everyone add block of transaction to blockchain.

- Private:

This type of blockchain allows only specific people in the organizations to add and verify transactions but other people can view the blocks.

- Consortium:

In this type, only a set of organizations can add and verify transactions. The ledger can be restricted or opened to selected group of people.

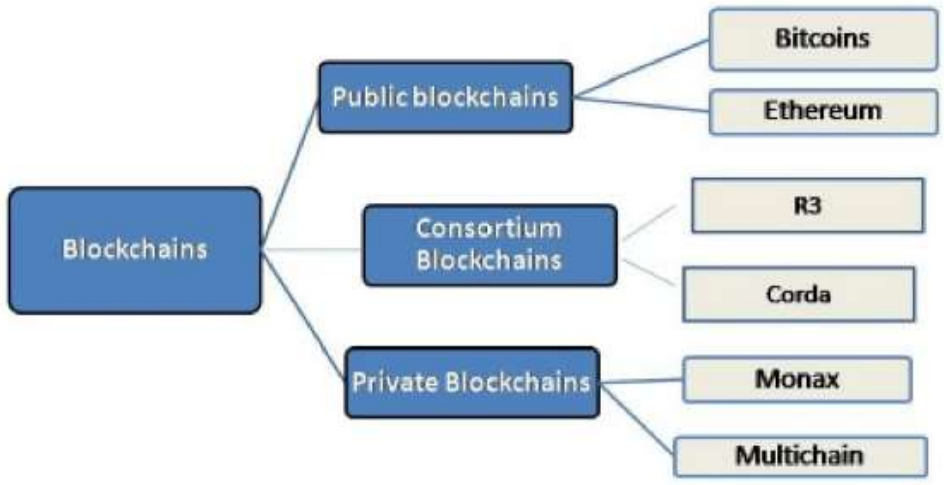

Fig 2: blockchain types

V. APPLICATIONS OF BLOCKCHAIN

- Supply chain management

Blockchain's immutable ledger makes it well-suited for tasks such as real-time tracking of goods as they move and change hands throughout the supply chain. Using blockchain opens up many options for companies transporting these goods. Entries on a blockchain can be used to queue events along the supply chain - for example, allocating goods arriving at a port for different shipping containers. Blockchain provides a new and dynamic means of organizing tracking data and using it.

- Healthcare

Health data appropriate for blockchain includes general information such as age, gender, and potential basic medical history data such as vaccination history or vital signs. By itself, none of this information will be able to specifically identify a particular patient, which allows it to be stored on a shared blockchain that can be accessed by many individuals without undue privacy concerns. As specialized connected medical devices become more common and increasingly connect to a person's health record, the blockchain can connect those devices to that record. The devices will be able to store data generated on the healthcare blockchain and can add it to personal medical records. A major problem currently facing connected medical devices is the siloing of the data they generate - but the blockchain may be the link that bridges those silos.

- Voting

Blockchain technology has the potential to make the voting process more easily accessible while improving security. Hackers will have no competition with blockchain technology, because even if someone accesses the terminal, they will not be able to affect other nodes. Each vote will be attributed to one ID, and with the ability to create fake IDs impossible, government officials can match votes more efficiently and effectively.

- Energy sector

According to PWC, blockchain technology can be used to execute energy supply transactions, and also to provide the basis for further metering, billing, and clearing processes. Other potential applications include documentation of ownership, asset management, basic guarantees, emissions allowances and renewable energy certificates.

- Payment processing

Probably the most logical use for blockchain is as a means of accelerating the transfer of funds from one side to another. As mentioned, banks have been removed from the equation, and most transactions processed on a blockchain can be resolved in a matter of seconds, with verification of transactions running seven days a week.

- Copyright and Royalty protection

In a world with increasing Internet access, copyright and ownership laws on music and other content have become blurred. With the blockchain, those copyright laws would be greatly extended to digital content downloads, to ensure that the artist or creator of the content being purchased gets their fair share. The blockchain can also provide transparent and real-time royalty distribution data to musicians and content creators.

V. CONCLUSION

Blockchain peer to peer (P2P) is a decentralized transaction and publicly available digital ledger. Bitcoin since 2008 And blockchain are one of the two most important technologies in information systems. Blockchain can be used for many applications to conduct transactions in a trustworthy environment without a third part. The research methodology is discussed following the architecture and working theory of blockchain. There are many areas where blockchain technology promises to solve the existing centralized system in a decentralized way. Several safety issues are also addressed. Studies have shown that some work is being done in terms of privacy and Security issues but a lot of reforms need to be done. Blockchain technology has many advantages such as decentralized, publicly available transactions, openness, secure. However, some research still needs to be done such as networks, Scalability and mining process of blockchain systems.

VI. REFERENCES

[1] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Fut. Gen. Comput. Syst. (2017), doi: 10.1016/j.future.2017.08.020

[2] M. Banerjee, J. Lee, K.K.R. Choo, A blockchain future to Internet of Things security: A position paper, Digit. Commun. Netw. (2017)

[3] B.A. Tama , B.J. Kweka , Y. Park , K.-H. Rhee , A critical review of blockchain and its current applications, in: Proceedings of the 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), IEEE, 2017, pp. 109–113.

[4] T.T.A. Dinh , J. Wang , G. Chen , R. Liu , B.C. Ooi , K.-L. Tan , Blockbench: a framework for analyzing private blockchains, in: Proceedings of the 2017 ACM
International Conference on Management of Data, ACM, 2017, pp. 1085–1100 .

[5] X. Min , Q. Li , L. Liu , L. Cui , A permissioned blockchain framework for supporting instant transaction and dynamic block size, in: Proceedings of the
2016 IEEE Trustcom/BigDataSE/I SPA, IEEE, 2016, pp. 90–96 .

[6] L. Luu , V. Narayanan , C. Zheng , K. Baweja , S. Gilbert , P. Saxena , A secure sharding protocol for open blockchains, in: Proceedings of the 2016 ACM
SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 17–30.

[7] R. Dennis , G. Owenson , B. Aziz , A temporal blockchain: a formal analysis, in: Proceedings of the 2016 International Conference on Collaboration
Technologies and Systems (CTS), IEEE, 2016, pp. 430–437 .

[8] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online].