IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

A Review Paper on Blockchain

Anish Kumar Kashyap
B. Tech (CSE) Student
Dronacharya College of Engineering, Gurgaon, Haryana, India

Abstract: *Blockchain being a number one technology within the 21st century is revolutionizing each sector of life. Services are being provided and upgraded using its salient features and fruitful characteristics. Businesses are being enhanced by using this technology. Countries are shifting towards digital currencies i.e., an initial application of the blockchain. It omits the necessity of central authority by its distributed a ledger functionality.*

Keywords: Blockchain

I. INTRODUCTION

The 21st century is all about revolutionizing technology. One among the leading teclmologies that has changed many aspects is blockchain. It impacted different businesses from the very initiative. Blockchain provides decentralized, transparent and secure systems. it's a distributed ledger technology which maintains a transaction ledger and secures it by using cryptography. The transactions are recorded in blocks and these blocks are connected to every other through hashes. Initially it had been employed by Satoshi Nakamoto in 2008 for public transactions of bitcoins. Bitcoin digital currency was the primary application of blockchain.

By definition, a blockchain may be a continuously growing chain of blocks, each of which contains a cryptographic hash of the previous block, a time-stamp, and its conveyed data. should be regenerated with new hash values. This feature of immutability is prime to blockchain applications. Operating a peer-to-peer network, it keeps records of the ledger of transactions. This helps to avoid any center party. the entire process is completed through a consensus. A ledger is shared between multiple entities, allowing everyone to examine it. No single user can control it. it's a distributed cryptographically secured database that keeps the record of each transaction from the very initial one.

II. TYPES OF BLOCKCHAIN

2.1. Public/Permissionless Blockchain

Blockchain that has no restriction on accommodating anonymous participants is understood as permissionless blockchain [26]. The term public blockchain is employed interchangeably. Lottery based consensus algorithms are wont to publish a block. one node is liable for publishing a block. Lottery-based mechanisms elect the validator to make a decision subsequent block to be added into the blockchain ledger. Election is predicated on a lottery draw and the one who wins is that the validator. Each new block is appended employing a new draw. The lottery-based mechanism avoids the malicious node having forged block to append it into the ledger. Such mechanisms don't follow a rule of thumb for electing the validator hence each lottery has its own trust model for electing the validator. Ifvoting based consensus is allowed to be utilized in permissionless blockchain, multiple accounts are often made by the participants to try to to a Sybil attack to form the choices in their favour. A sybil attack is one among the difficulty in peer to see network where a malicious node creates many identities and tries to control the network by controlling it. Public blockchains need security and for this purpose the block creation mechanism must be difficult and expensive in order that the resources of 1 node aren't enough to bias the choices in its favor. The disadvantage of public blockchain is in terms of PoW where heavy computation power is required . All the nodes got to solve a cryptographic puzzle by brute force. The node which wins the puzzle is rewarded and every one the opposite nodes computations are wasted. The consensus is achieved as 51% of power. Proof of stake uses the wealth of miners to win a ticket instead of computational power.

2.2. Private/Permissioned Blockchain

Private blockchains, which can even be mentioned as managed blockchains, are permissioned blockchains controlled by one organization. during a private blockchain, the central authority determines who are often a node. The central authority

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

also doesn't necessarily grant each node with equal rights to perform functions. Private blockchains are only partially decentralized because public access to those blockchains is restricted. Some samples of private blockchains are the business- to-business virtual currency exchange network Ripple and Hyperledger, an umbrella project of open-source blockchain applications. Both private and public blockchains have drawbacks - public blockchains tend to possess longer validation times for brand spanking new data than private blockchains, and personal blockchains are more susceptible to fraud and bad actors. to deal with these drawbacks, consortium and hybrid blockchains were developed.

2.3. Hybrid Blockchain

A hybrid blockchain combines the privacy of a private blockchain with the safety and transparency of a public blockchain. this provides the companies a big amount of options to settle on from for what they need to stay private and what to be made public. for instance , real-world application of hybrid blockchains includes Ripple network and therefore the XRP token. It allows its users to attach with other blockchain protocols. Thus, allowing blockchains multichain network. This functionality makes it simple for businesses to work with the transparency they're trying to find , without having to sacrifice security and privacy. having the ability to post to multiple public blockchains directly increases the safety of transactions, as they enjoy the combined hash power being applied to the general public chains

III. BLOCK CHAIN ARCIDTECTURE

The initial block during a block chain is understood because the genesis block. A genesis block doesn't contain a previous hash but its own hash. Figure 1 shows a general view of a blockchain. A block contains the transactions, hash of the previous block and hash of subsequent block. This information is stored during a block using cryptographic techniques. A block within the chain can come from any current block. Thus a miner creates the chain of blocks, the hash of the previous is added to added to the present block. Thus the miner creates a replacement block by using the discuss of it. this manner a replacement block is made . This recently formed block now end up to be the new end for the chain. By this mechanism the chain grows as more blocks are added by the miners.

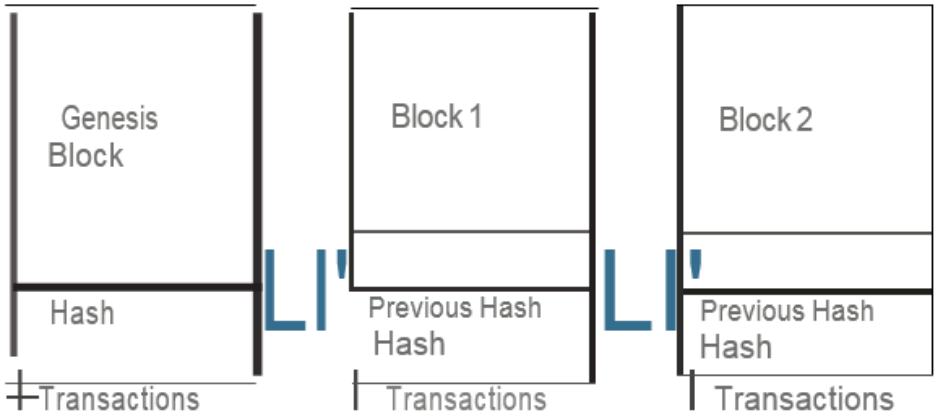

Figure 1: Blockchain Architecture

IV. CONSENSUS ALGORITHMS

A consensus algorithm may be a technique through which all the peers of the blockchain network reach a standard agreement about the present state of the distributed ledger. Therefore, consensus algorithms provide trust and reliability among unknown peers during a distributed environment. A consensus mechanism ensures that each new block added to the blockchain is that the only truth which is prescribed by all the blockchain nodes.

The blockchain consensus protocol comprises some specific aims that are coming to an agreement, co-operation, collaboration, mandatory participation of every node within the consensus process and equal rights to each node. Hence, a consensus algorithm targets at finding a standard agreement that's a win for the entire network. The above discussed applications are categorized and consensus algorithms supported these categories are further discussed below. Figure 2 shows a categorical diagram of the consensus and their distribution.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

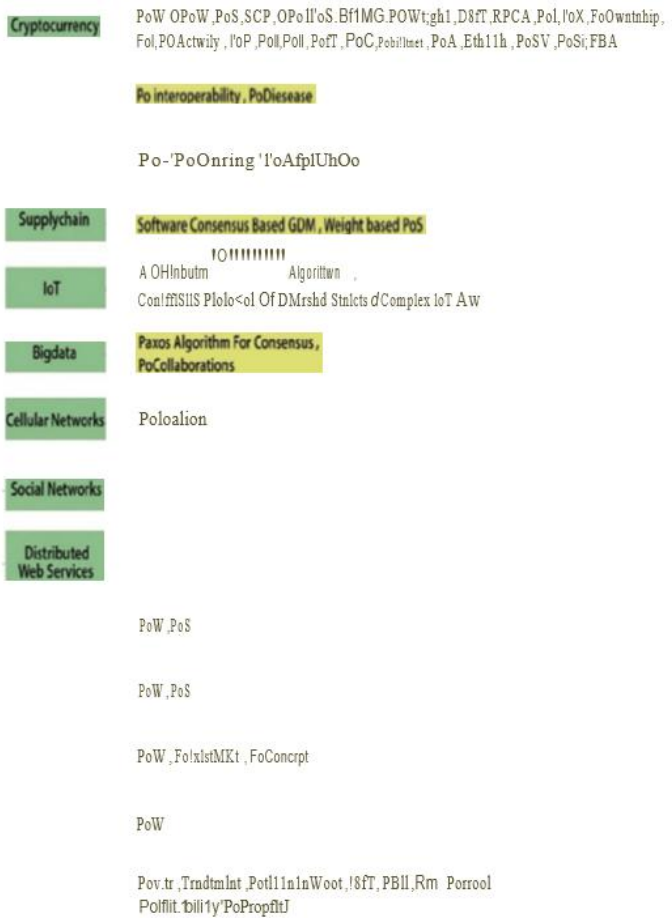

Figure 2: Categorization of Consesnsus Algorithms

V. APPLICATION OF BLOCK CHAIN

Beyond the currency setting, there are other uses for blockchain too. Its underlying technology is used in various applications. Figure 3 shows the various applications of blockchain. Some of the applications of blockchain is listed below.

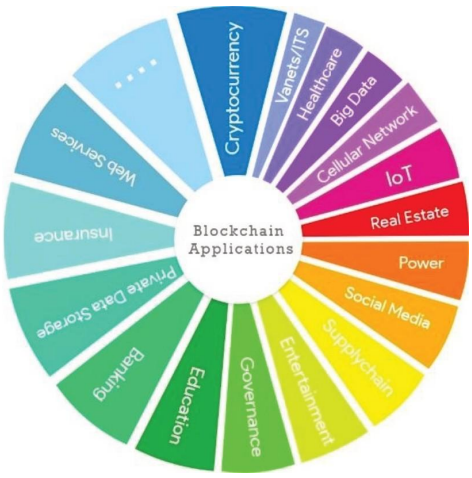

Figure 3: Application of Blockchain

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

5.1 Cryptocurrency

Over the past decade cryptocurrency is being an evolving topic, merging incredible technical power and enticing investments worth useful trillions dollars on a world wide scale. The underlying technology of cryptocurrency is attractive for several other applications thanks to its unique features and architecture. this is often why it's becoming popular thanks to its applicability, efficiency and data-centric characteristics [35]. Cryptocurrencies like bitcoin use blockchain technology to secure transactions using hashes. Bitcoin was the primary cryptocurrency using blockchain with Proof of labor algorithm

5.2. Supply Chain Monitoring

Using blockchain technology to trace items as they move through a logistics or supply chain network can provide several advantages. First of all, it provides greater simple communication between partners since data is out there on a secure public ledger. Second, it provides greater security and data integrity since the info on the blockchain cannot be altered. meaning logistics and provide chain partners can work together more easily with greater trust that the info they're provided is accurate and up so far .

5.3. Internet of Things (IoT)

The Internet of Things (IoT) may be a network of connected vehicles, home appliances, physical devices, and other items that are accessible through the web . IoT is widely utilized in smart homes, smart grid, intelligent manufacturing, intelligent transportation , and other fields. the normal centralized network doesn't guarantee trusted interaction among devices and security of sensitive information. Therefore, the mixture of blockchain and IoT is an expected trend, where smart contracts will help to automate, promote resource sharing, complex workflow, ensure safety, efficiency and save costs. a sensible home model is proposed by Dorri et al which is predicated on blockchain and smart contracts. They discussed how through simulations the value of daily management ofioT devices are often reduced. They also discussed within the model, various interaction processes.

5.4. Healthcare

Healthcare is moving towards digitization with an increased number of hospitals, doctors, healthcare machinery to record patient's record digitally. Digitization of med- ical data allows sharing and retrieval easily for deciding purposes. However such digitization is risky in terms of patient privacy violation. A blockchain-based Healthcare Data Gateway (HDG) was proposed by Yue et al. They used a personal blockchain cloud to ensure that the medical data can't be changed by anybody including the patient himself and/or the physicians. A blockchain-based interoperable Electronic Health Record (EHR) framework proposed by provides important reliability and security re- quirements. It enables different organizations of variant internal structures to speak with one another using the prevailing EHR infrastructure of organizations.

5.5. Voting

In the year 2014, a Danish party was the primary to use blockchain technology for voting. 'Followmyvote' offers a web voting platform which follows blockchain technology for secure electoral system. A challenge for fair electoral system which keeps users' voting privacy which provides transparency and adaptability of electronic system is solved during this paper. a completely unique blockchain application for fair electronic voting is proposed by [50] which eliminates a number of the prevailing systems issues. It particularly addresses the election process which reduces the value of conducting elections nationwide

REFERENCES

[1]. Yang, X., Chen, Y., & Chen, X. (2019). "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information." 2019 IEEE International Conference on Blockchain (Blockchain).

[2]. Yu, S., Lv, K., Shao, Z., Guo, Y., Zou, J., & Zhang, B. (2018). A High Performance Blockchain Platform for Intelligent Devices. 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN).

[3]. Zheng Z, Xie S, Dai H, et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends[C]. IEEE International Congress on Big Data. IEEE, 2017.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

[4]. Ribeiro, S. L., & de Paiva Barbosa, I. A (2020). Risk Analysis Methodology to Blockchain-based Solutions. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)

[5]. Sahnan, T., Jain, R., & Gupta, L. (2019). A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains. 2019 IEEE International Conference on Blockchain (Blockchain).