International Journal of Research in Advent Technology, Vol.8, No.12, December 2020
E-ISSN: 2321-9637
Available online at www.ijrat.org

Public Distributed Decentralized System as Blockchain

Sayali Sandesh Pingale, Prof. Rohit Bag, Dr. Mangesh M. Ghonge

Abstract— Blockchain technology is very useful in multiple areas in our day-to-day world. Along with many social networking platforms there is a possibility of data theft or tampered or data leakage and hence we need our data to be secure and immutable. One of the best solutions to this problem is blockchain technology. It replaced the traditional centralized system with a distributed, decentralized database system. A centralized system requires third parties like servers, banks, or any intermediary for transactions between two users where decentralized systems do not require any central authority to work in between two users. Blockchain technology fully works on a decentralized system. By using a cryptographic consensus algorithm, we achieve privacy, security, and immutability. This paper presents the survey of the most important technology, also presents prerequisites of the technology. The purpose of this paper is too familiar with the innovative, revolutionizing technology as well as awareness of the technology. This paper gives an idea of whether we choose blockchain or not as the right solution for our application based on its characteristics, design, and implementation.

Index Terms— Blockchain, bitcoin, ethereum, smart contracts, PoW, and PoS.

I. INTRODUCTION

There is a question, why we need blockchain? Imagine A and B are two friends living far away and want to transfer money to each other. To transfer the money, they rely on a third party on which they have trust. Besides, what will be the possible results by doing this way in transactions? There are high transaction fees associated with it. For any transaction, the bank will charge a high amount of transaction fees. There could be internet-based frauds, hackers attack financial institutions and gain unauthorized access to steal money or any type of assets. There could be poor data recovery. Also, retrieving lost data is very difficult in a centralized system. But as compared to the distributed databases, distributed ledger technology like blockchain is easy as that information is distributed across multiple nodes. Now, these problems can be solved using blockchain technology.

Manuscript revised on December 19, 2020 and published on January 10, 2021
Sayali Sandesh Pingale, *Sandip Institute of Technology and Research Center, Nashik, Maharashtra, India*
Prof. Rohit Bag, *Sandip Institute of Technology and Research Center, Nashik, Maharashtra, India*
Dr. Mangesh M. Ghonge, *Sandip Institute of Technology and Research Center, Nashik, Maharashtra, India*

Blockchain is a decentralized, distributed, public ledger system [4]. It can be described as a collection of records; linked with each other; robust resistant to alteration; protected using cryptography. A hacker will not be able to alter the data in the blockchain because each user has a copy of all the records, the data within the blocks are encrypted by algorithms. All of this is made possible with the help of blockchain technology. The concept of a blockchain that ensures records are immutable means cannot be altered by any of the users within the network through a public distributed ledger, proof-of-work, proof-of-stake, and cryptographic hash encryption. This paper presents the importance of blockchain technology, presents prerequisites that need to know for the implementation of the technology.

II. BACKGROUND

In 2008, firstly the blockchain technology was proposed by a person (or group of peoples) named Satoshi Nakamoto [1], who invented the first digital cryptocurrency known as bitcoin. Bitcoin aimed to solve the problems faced by fiat currencies, with the help of blockchain technology. The transaction details are permanently inscribed in the block of the blockchain. It does not need a central authority that is a third party. It is fully based on a decentralized, distributed ledger. Bitcoin works on peer to peer decentralized network known as a distributed system. Every user in the bitcoin network has two keys one is private, another is a public key because of this, we achieve confidentiality and authentication. The public key can be visible to all the users in the network, the private key is a unique address that the only user knows of. Bitcoin uses a cryptographic algorithm SHA-256 where ethereum uses ethash.

III. PUBLIC V/S PRIVATE BLOCKCHAIN

A. Permissioned /private Blockchain

A private blockchain is a permissioned blockchain. They certainly allowed participants in the network access the permissioned block. It can be called as an additional blockchain security system. Authorized participants have done the verification of transactions of the permissioned blockchain. One or more entities have the right to handle, read, and write the contents of the transactions in the block, whereas other entities will not be able to access it. The ledger does not require a consensus algorithm to ensure tamper resilience. Hyperledger Fabric and R3 Corda are examples of the permissioned blockchain [6].

B. Permissionless/public Blockchain

A public blockchain is a permissionless blockchain. It is open to all participants in the network. Anyone could be joined the network, there are no restrictions on accessing the

doi: 10.32622/ijrat.812202003

transaction. Anyone can have the rights to update the transaction, view the contents of the block. For security, the ledger requires the cryptographic consensus algorithms, to help to design the structure of the permissionless blockchain. Data on a public blockchain are secure as it is not possible to modify or alter, once they have been validated on the blockchain. Bitcoin and Ethereum are examples of a permissionless blockchain [1].

IV. ARCHITECTURE

A. Cryptographic algorithms for Hashing

In the Hashing technique, an arbitrary length of data provided as an input to hash function which produces the hash value of a fixed length [3]. Fixed hash is based on the algorithm which has been used in the hashing. Once the hash value is generated it cannot reverse back to the actual input value. Every different input has a unique hash. In case, two inputs generate the same hash then the collision occurs. SHA-256 algorithm, SHA-512 algorithm is used for hashing technique. A cryptographic hash is like a signature for a text or a data file. SHA-256 algorithm generates a unique, fixed-size 256-bits hash [1]. Cryptographic hashes have maintained data integrity in the blockchain.

B. Consensus

If the participants are done some transactions, a new block is created from that transactions and there is a necessity to securely store it in the blockchain. So who will add it to the chain is defined by the consensus algorithm. The consensus is also used to identify the validation of the transaction, checks maliciousness as well. If the consensus is based on proof-of-work, each participant starts finding the appropriate proof-of-work. Based on permissions or permissionless blockchain we have different consensus algorithms.

C. Proof-of-Work (PoW)

PoW is the consensus algorithm responsible for building a new block on the blockchain through the computational hashing power competition among the nodes. The node who won the competition has the right to link block to the chain as well as achieve rewards. It is the consensus algorithm used in bitcoin [6].

D. Proof-of-Stake (PoS)

PoS is one of the consensus algorithms used in digital currencies. Like the proof-of-work algorithm, PoS not spend the number of computational power resources. The node who has the potential to investing cryptocurrencies will have more stake means have more right to build a new block on the blockchain.

V. ETHEREUM

Ethereum is a decentralized, public, open-source platform on the blockchain network which has a prominent concept of smart contracts [4]. It is a platform where decentralized applications were created known as Dapps. Ethereum was invented by Vitalik Buterin. It is come up with an innovation that opened the door of executing many different ideas over the blockchain is a decentralized Turing Complete Virtual Machine known as EVM (Ethereum Virtual Machine) [3][4]. EVM is used to run the software, applications on the blockchain. Ethereum has its digital cryptocurrency named Ether. Ether is used to pay for the computational resources and the transaction fees on the ethereum network.

Smart Contracts

A smart contract is a simple computer program that facilitates to exchange of any valuable assets between two users. By the use of the Ethereum network, we can write the programming codes if those codes represent any type of contract called smart contracts. They are self-enforcing contracts written into lines of code. It is proof of transactions carried out among anonymous participants without the need for a central authority to be trusted and transparent. The cryptocurrency ether has the capability of powers the programmable smart contracts [5]. They render transactions traceable, transparent, and irreversible [4].

VI. DESIGN

In the bitcoin blockchain, after there are done some transactions, the block is mined by miners and updates the blockchain. Before uploading the block on the blockchain, they will compete with each other by doing the computational work called proof-of-word [3]. And who will succeed the competition of consensus can upload the block in the blockchain network and get rewards by means will achieve security. Block in the blockchain has transactions contains with block header.

The Block header holds the timestamp to know when the block was created, and also, the version which we used. It contains the Merkle root is the one hash of all n number of transactions of the block. It also carries difficulty target and nonce. Block header contains a hash of its previous block. Every block generates its hash value by hashing technique. Fig. 1 shows a block header.

Fig. 1 Block Header

Fig. 2 shows the hashing of peer to peer network of the blockchain. Blocks are connected in chronological order to each other. In the blockchain, the first block is a genesis block. The hash value of block 1 is H1 is present in the next block that is block 2. Similarly, the hash value of block 2 is H2 is present at block 3. The hash value of the previous block should present in the current block [3]. By hashing technique, data would be secured because if anyone tried to change the hash of a block, ultimately the hash value changes of all

doi: 10.32622/ijrat.812202003

blocks. And it cannot be possible at any cost. So, our data will be secured by using a hashing technique.

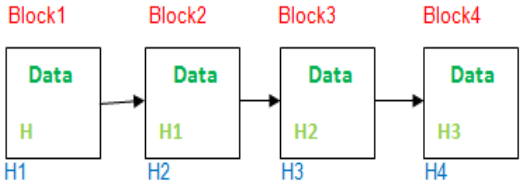

Fig. 2 Blockchain Hashing Technique

VII. APPLICATIONS

Blockchain technology spread in the various fields by its features or its characteristics. Blockchain technology also has the potential to disrupt the insurance industry [6]. It is applicable in the fields like Finance Services, the Internet of things (IoT), Smart Healthcare, Smart Government, and many more. Following there is some applications are given below:

- In the field of Finance Services, blockchain provides a new way of managing trust and can be effectively applied in insurance and domains like finance [2], it is useful for asset management, insurance claims processing, and also for Cross-Border Payments.
- In the field of Smart Property, it is useful for the Money Leading, Smart Car, and Smart Phone.
- In the field of Internet of Things (IoT), blockchain eliminates the usage of centralized devices the IoT [2], it is useful for the Smart appliances, and Supply chain sensors.
- In the field of Smart Healthcare, It is envisioned that the blockchain can have significant applications in smart healthcare with the Internet of Medical Things (IoMT) or the Internet of Health Things (IoHT) [2], it is useful for the Personal Health Record-Keeping, Access Control, Healthcare Management, and Insurance Processing.
- In the field of Smart Government, it is useful for the Electronic Passport, Birth certificate, Wedding Certificates, and so on, Personal Identification, and Smart Community.

VIII. CONCLUSION

Blockchain is the technology that is needed for various rationales to the industries. More and more companies are realizing the revolutionary potential of this technology by knowing its characteristics, and are looking to leverage it for their daily operations. Blockchain is a platform for sharing information across the globe that cannot be manipulated or changed through cryptographic hashing technique, consensus algorithms like proof-of-work, proof-of-stake. It follows a community-verified work system. And my motive to publish this review paper is to readers should be aware of this technology, and they should be taken the benefits of the technology to build their application or software based on this useful blockchain technology.

REFERENCES

[1] Ms. Sheetal, and Dr. K. A. Venkatesh, *Necessary requirements for Blockchain Technology and its Applications*, International Journal of Computing Science and Information Technology, 2018, *ISSN: 2278-9669, April 2018 (http://ijcsit.org).*
[2] Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Chi Yang, *The Blockchain as a Decentralized Security Framework.*
[3] Sherif F. Fahmy, *Blockchain and its uses,* Sherif F. Fahmy is a lecturer in the Arab Academy for Science and Technology and Maritime Transport, Sheraton, Cairo, Egypt (phone: 01224469125; e-mail: fahmy@aast.edu). January 18, 2018.
[4] Keyur Paralkar, Shiwani Yadav, Shikha Kumari, Apurva Kulkarni, S.P. Pingat, *Photogroup: Decentralized Web Application Using Ethereum Blockchain*, International Research Journal of Engineering and Technology (IRJET), *e-ISSN: 2395-0056*, Volume: 05 Issue: 04 | Apr-2018 *www.irjet.net*, p-ISSN: 2395-0072.
[5] Abhishek Jain, Aman Jain, Nihal Chauhan, Vikrant Singh, Narina Thakur, *Seguro Digital storage of documents using Blockchain*, International Research Journal of Engineering and Technology (IRJET), *e-ISSN: 2395-0056*, Volume: 05 Issue: 04 | Apr-2018, *www.irjet.net*, p-ISSN: 2395-0072.
[6] Hoang Tam Vo, Ashish Kundu, Mukesh Mohania, *Research Directions in Blockchain Data Management and Analytics.*
[7] Bektur Ryskeldiev, Yoichi Ochiai, Michael Cohen, Jens Herder, *Distributed Metaverse: Creating Decentralized Blockchain-based Model for Peer-to-peer Sharing of Virtual Spaces for Mixed Reality Applications.*
[8]https://www.simplilearn.com/what-is-blockchain-technology-and-how-does-it-work-article
[9] https://en.wikipedia.org/wiki/Blockchain
[10] https://blockgeeks.com/guides/ethereum/
[11] http://blockchainhub.net/smart-contracts/
[12]https://www.intheblack.com/articles/2018/09/05/difference-between-private-public-blockchain
[13] https://www.investopedia.com/terms/p/permissioned-blockchains.asp
[14] https://www.quora.com/What-is-blockchain-technology-1
[15]https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/#:~:text=A%20consensus%20algorithm%20is%20a,state%20of%20the%20distributed%20ledger.&text=Thus%2C%20a%20consensus%20algorithm%20aims,win%20for%20the%20entire%20network.
[16]https://medium.com/@MLSDevCom/blockchain-architecture-basics-components-structure-benefits-creation-beace17c8e77
[17] https://www.edureka.co/blog/blockchain-architecture/
[18] https://blockgeeks.com/guides/blockchain-consensus/

doi: 10.32622/ijrat.812202003