Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 22 Issue 1, January 2020

Review Paper on Blockchain and Its Current Applications

Dr. Abhishek Kumar, Dr. S.S. Chauhan, Mr. Somprabh Dubey
Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- abhishekkumar@shobhituniversity.ac.in, sschauhan@shobhituniversity.ac.in,
sompradb.dubey@shobhituniversity.ac.in

ABSTRACT: Since the advent of Bitcoin, the first and biggest cryptocurrency, blockchain technology has been recognized as a digital currency platform. It has previously been used for decentralization of markets in general, rather than just independence of currency and transactions. The blockchains distributed transactional ledger may be used to register, confirm, and transmit various types of contracts to other network participants. We fully examine state-of-the-art blockchain-related applications that have appeared in the literature in this article. A software application may be categorized as either centralized or distributed, depending on its architectural approach. A centralized software system's nodes are dispersed and connected to a single central coordinating node. A distributed system, on the other hand, is made up of numerous linked nodes that are controlled by a single point. A distributed system offers a number of benefits, including increased processing power by pooling the computing capability of all linked nodes, better dependability due to the absence of a single point of failure, and so on. A number of previously published publications were carefully considered for inclusion based on their addition to the blockchain body of knowledge. In the last part of the article, many points are examined and debated.

KEYWORDS: Blockchain, Cryptocurrency, Currency, Network, Software.

1. INTRODUCTION

A software system may be classified into one of two architectural approaches: centralized or distributed. The nodes of a centralized software system are spread out and linked to a single central coordinating node. A distributed system, on the other hand, consists of many interconnected nodes with no single point of control. A distributed system has many advantages, including greater processing power by pooling the computing capacity of all connected nodes, improved dependability owing to the lack of a single point of failure, and so on. However, there are many disadvantages to a distributed system, including communication cost and security concerns linked to untrustworthy nodes abusing network access[1].

Meanwhile, blockchain may be seen as a component of a distributed software system's implementation layer. Blockchain may be used to achieve and preserve data integrity in distributed systems. Furthermore, blockchain may be thought of as a solely peer-to-peer system composed of individual nodes in a network. In peer-to-peer networks, dishonest and malevolent peers constitute the most serious integrity threat. Because unknown peers with uncertain dependability and trustworthiness may exist, individual nodes attempt to abuse the system for their own objectives. As a result, blockchain is required to address these important issues[2].

Bitcoin, along with blockchain, was created by Nakamoto as the first and most widely used cryptocurrency. It allows for trust-less and reliable transactions without the need for centralized administration, even when users do not trust each other or the network contains untrustworthy individuals. Since then, blockchain has attracted a lot of interest for its decentralized transaction ledger capability, which can be used to register, confirm, and transmit payments or contracts. Furthermore, blockchain technology has been used to transactions and uses beyond than financial transactions, including as healthcare, utilities, real estate, and government. These are proven possible since the Bitcoin blockchain structure is portable and extendable[3].

Initially, blockchains primary use was to link cryptocurrencies to traditional banking and financial institutions. Blockchain technology creates a new banking environment, allowing financial institutions to conduct transactions directly amongst themselves without the need for central authorities or intermediaries. Every transaction must be verified by the consent of more than half of the network's participants. This implies that no participant may change any data on the blockchain without the permission of other participants[4].

The purpose of this article is to offer and examine information on blockchain technology and its current uses in the real world. The document categorizes published works in the literature, such as academic journals, conferences, technical reports, and so on. Most studies, on the other hand, have not included a thorough examination of blockchain-related applications. The remainder of the paper is organized in the following manner[5].

1.1 Blockchain Technology Fundamentals:

Blockchain is a kind of distributed ledger (data structure) that stores transaction or event information. It is copied and shared across the network's members. Since blocks are added to the chain, its size continues to grow. Figure 1 shows the Centralized and distributed network architecture.

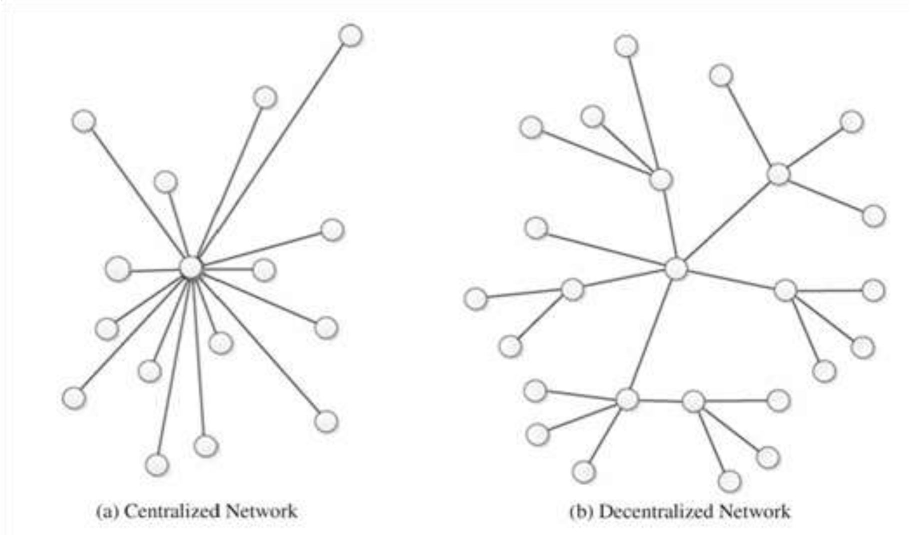

Figure 1: The above figure shows the Centralized and distributed network architecture[1]**.**

Utilizing a hash function to be added and linked to the preceding block. To generate a hash, a cryptographic hash function is needed. Bitcoin, for example, employs the SHA-256 algorithm, while lite coin and Prime coin use the Script and Cunningham chains, respectively. It also allows us to quickly check the input mapping to a particular hash value. It would be impossible to have the same hash for two distinct inputs.

A network node (user) validates and preserves the ledger on the blockchain using a consensus mechanism (a set of rules that allows users to achieve a mutual agreement), eliminating the need for a central authority or intermediary. Each node maintains a full copy of the ledger. Section III delves into the practical application of blockchain for financial transactions, since the primary goal of blockchain is to address the issues that present in the Bitcoin cryptocurrency. Figure 2 shows the chain of blocks - blockchain in the Bitcoin.

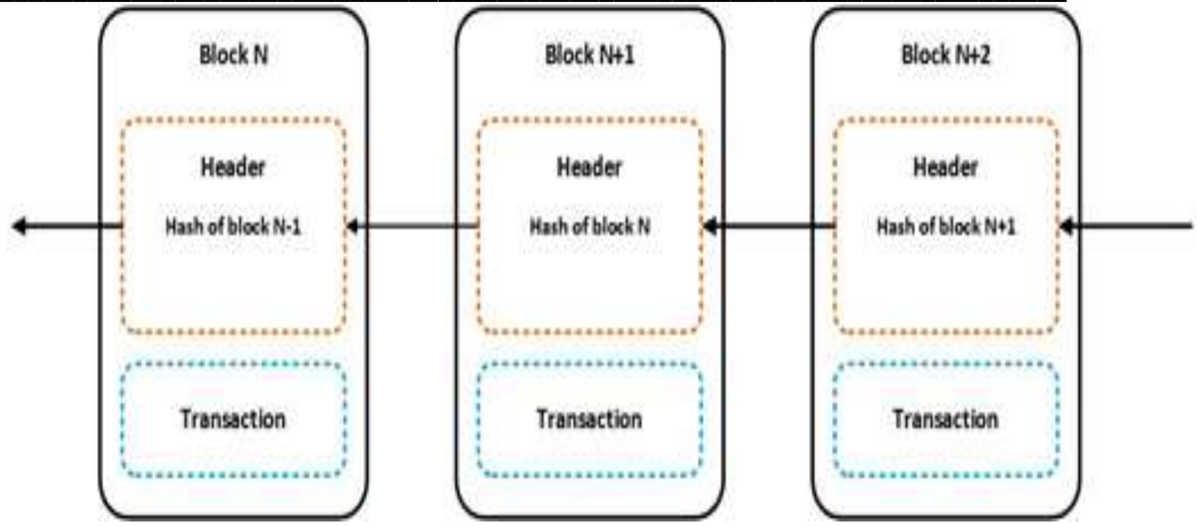

Figure 2: The above figure shows the chain of blocks - blockchain in the Bitcoin[1]**.**

1.2 Applications of the Blockchain:

The use of blockchain technology in many fields is extensively explored in this section. Furthermore, financial services, healthcare, business and industry, and other new applications have all been classified as such applications.

1.2.1 Financial Services:

The blockchain technology has been extensively used for financial transactions, or cryptocurrencies. Cryptocurrencies have become popular software systems in recent years. The first block's hash is sent to the miner, who uses it to create the second block's hash. Similarly, the third block generates a hash that includes the previous two blocks, and so on. The genesis block may be traced back to all other blocks on the blockchain[6].

Cryptocurrency has its own monetary system (coin). The process of adding a new block to the blockchain is known as mining. Each node checks the blockchain to see whether the currency is genuine and has not been spent yet. A larger number of parties must agree before the transaction records are added to the blockchain. Because the mining process consumes many resources, it is difficult for an attacker to verify an incorrect transaction. Each mined block is examined to see if it contains a legitimate proof of labor or a proof of stake[7].

The common stages in cryptocurrencies are as follows:

- For a user with a wallet, a created address (public key) is accessible.
- A private key is allocated to the wallet. It is used to sign transactions and prove ownership.
- The payer transfers currency to the payee using the provided address and signs it with the payer's private key.
- The transaction is verified via the mining process.

Bitcoin, Litecoin, Peercoin, Primecoin, Ripple, Ethereum, Permacoin, Blackcoin, Auroracoin, Darkcoin, and Namecoin are the eleven cryptocurrency systems studied. The aforementioned cryptocurrency systems.

1.2.2 Medical Care:

Blockchain holds a lot of promise in terms of resolving the interoperability problems that plague today's healthcare systems. It may be used as a standard to enable stakeholders, such as healthcare entities, medical researchers, and others, to securely exchange electronic health records (EHRs). For example, sharing EHR allows us to improve the quality of medical treatment and improve doctor recommendations.

However, managing healthcare data, that is, collecting, keeping, and analyzing it, is not an easy job, especially when privacy concerns are involved. Healthcare information should not be shared with anyone else since malicious users or attackers may use it fraudulently. A healthcare data gateway (HDG) based on the blockchain storage technology in order to address these problems. It is a smartphone application that allows users to simply manage and restrict data sharing. Users may process patient data using the suggested approach without jeopardizing patient privacy. Furthermore, the data is kept in a private blockchain cloud, guaranteeing that medical data cannot be tampered with by anybody, including doctors and patients[8].

The study focuses on the creation of a new system called MedRec that prioritizes patient agency. Blockchain is a distributed ledger system that employs public key cryptography. Each node in the network receives a copy of the blockchain. Blockchain technology is utilized as an access control in order to automate and monitor specific actions, such as appending a new record, changing viewing rights, and so on, similar to previous work. Smart contracts on the Ethereum blockchain are also used to construct sophisticated representations of EHR that are kept in each node.

Following that, proposes utilizing blockchain to implement pervasive social network (PSN)-based healthcare. We can exchange medical data collected by medical sensors via PSN. The authentication protocol between medical sensors and mobile devices in a wireless body area network (WBAN) and the EHR data exchange utilizing blockchain in the PSN area are the two primary security protocols in a PSN-based healthcare system. Medical data transactions, such as node address and medical sensors, are generated and broadcast by each node in the PSN. The miners, on the other hand, are in charge of transaction verification and the production of new blocks[9].

Finally, proposes a blockchain-based access control system. Identification, authentication, and permission are all part of the access control process. It establishes a state of accountability in which user access can be tracked for what specific activity in a system. After confirming their identity and cryptographic keys, users may obtain EHR from shared data pools using the proposed approach. Identity-based authentication is used to accomplish user authentication. In addition, a lightweight block structure is suggested to improve the existing blockchain implementation[10].

1.2.3 Industry and Business:

The rise of the Internet of Things (IoT) has offered numerous benefits, including the ability to link things and people. This prompts the authors of to propose an e-business architecture tailored to the IoT context. The distributed autonomous corporation (DAC) as an organization for this purpose. The proposed system's main component is a transaction mode in which peer-to-peer transactions are carried out autonomously, with Bitcoin and IoTcoin serving as the currency and exchange certificate, respectively.

When proposing an agri-food supply chain traceability system utilizing RFID and blockchain technologies, the authors emphasize the significance of food safety and quality. Blockchain is used to ensure that information exchanged and published is accurate and trustworthy. Furthermore, in the age of Industry 4.0, the term 'smart manufacturing' is widely explored in. Industry 4.0 refers to the ability of goods and services to be shared across networks, such as the Internet or blockchain. In terms of supply chain management, Industry 4.0 is anticipated to bring decentralization and self-regulation to the fore.

Too far, writers have been drawn to a kind of cloud computing known as fog computing or edge computing in order to create a fair payment system based on Bitcoin. Fog computing is a large-scale, pervasive, and decentralized computing system that can handle any computer job. The suggested method aims to improve on the conventional electronic currency system, which requires a trusted entity, such as a bank, to issue payment tokens. By using Bitcoin-based payment, fog users (outsourcers) may send money directly to fog nodes (workers) without the need for a third party. The authors claim that regardless of whether the outsourcers are malevolent or not, the suggested method can guarantee payment for any completed activities done by honest employees.

1.2.4 Additional Implementations:

The present application of blockchain in a variety of domains, including right management, reputation, digital content distribution, WiFi authentication, and IoT security, is addressed in this section.

The two articles introduce and explore a novel decentralized right management system based on blockchain technology (BRIGHT). This is in stark contrast to the conventional method, which often involves a central third party. The suggested system is anticipated to feature a robust anti-attack mechanism and will allow us to reduce customer service costs. Furthermore, a reputation system has many possibilities for assessing our community's trustworthiness. It is calculated using our past transactions and interactions in a network, such as an e-commerce website. By incorporating blockchain into the reputation system, it will be possible to address the main problems that now exist in the system, such as freeloaders.

A new authentication protocol for WiFi. This is based on Bitcoin 2.0, which is a Bitcoin-based alternative currency system. Users must first download and install the Auth-Wallet program, after which Auth-Coins are provided. Tokens are exchanged between users and access points for authentication. Finally, describes the application of blockchain for smart home security. A private and local blockchain is used to offer secure access control to the IoT devices. The blockchain not only provides a lightweight security mechanism for smart home devices, but it also creates an immutable time-ordered database of transactions. In addition, a smart home miner is a device that processes transactions in the smart home from a central location. Figure 3 shows the Paper distribution by year.

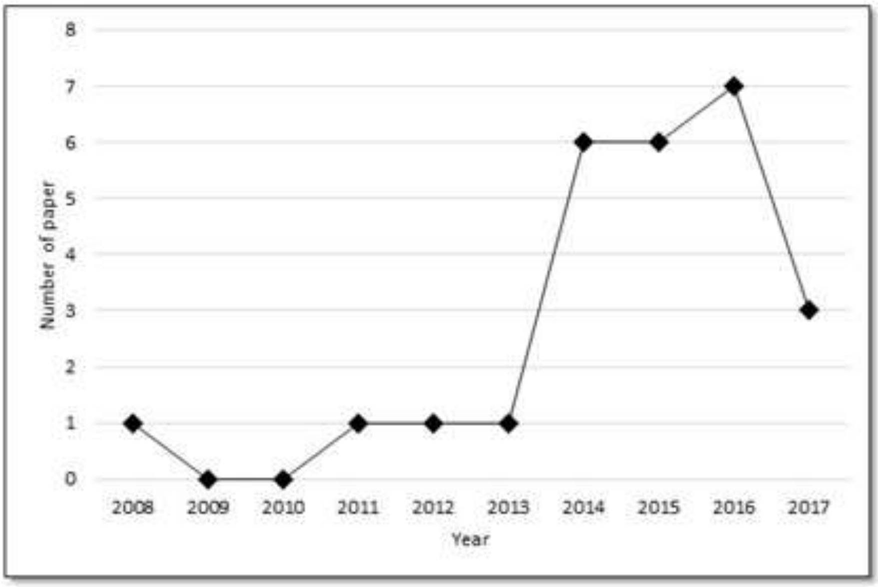

Figure 3: The above figure shows the Paper distribution by year[1].

2. DISCUSSION

The author has discussed about the blockchain and its current applications. It has previously been used for market decentralization in general, rather than simply currency and transaction independence. The distributed transactional ledger of the blockchain may be used to register, confirm, and transmit different kinds of contracts to other network members. In this essay, we thoroughly analyze state-of-the-art blockchain-related applications that have emerged in the literature. Depending on its architectural style, a software program may be classified as centralized or distributed. The nodes of a centralized software system are distributed and linked to a single central directing node. A distributed system, on the other hand, is made up of many interconnected nodes that are all managed from a single location. Increased processing capacity by pooling the computational capabilities of all connected nodes, greater dependability owing to the lack of a single point of failure, and so on are some of the advantages of a distributed system.

3. CONCLUSION

The most recent state-of-the-art research articles on bitcoin blockchain were examined and debated. A number of articles were carefully selected from an internet database and then categorized into various categories. This article provides an overview of current cryptocurrency research as well as real-world applications. Nakamoto developed Bitcoin, along with cryptography, as the first and most extensively used cryptocurrency. Even when users do not trust each other or the network includes untrustworthy people, it enables for trust less and reliable operations without the requirement for centralized management. Blockchain is a separate economic model from the rest of the world (coin). Mining is the act of putting a new block on the blockchain. Each node examines the network to verify whether the money is valid and has not yet been spent. Prior to transaction information being uploaded to the database, a greater number of participants must agree. Since then, blockchains decentralized transaction ledger capabilities, which can be used to register, confirm, and transfer payments or contracts, has piqued attention.

REFERENCES

[1] B. A. Tama, "<08167115.Pdf>," pp. 109–113, 2017.

[2] A Tilooby, "The Impact of Blockchain Technology on Financial Transactions," *August 14*, 2018.

[3] P. S. M. K. Alex Kibet, "A Synopsis of Blockchain Technology," *Int. J. Adv. Res. Comput. Eng. Technol.*, 2018.

[4] T. Thurner, "Supply chain finance and blockchain technology – the case of reverse securitisation," *foresight*, 2018, doi: 10.1108/fs-08-2018-099.

[5] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl. Energy*, 2017, doi: 10.1016/j.apenergy.2017.03.039.

[6] P. R. Newswire, "Global Blockchain Technology Industry," *NY-Reportlinker*, 2018.

[7] B. K. Mohanta and D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)," *2018 9th Int. Conf. Comput. Commun. Netw. Technol.*, 2018.

[8] D. M. Kayam, "Blockchain Technology: An Approaching Game Changer in Financial Service Industry," *Int. J. Trend Sci. Res. Dev.*, 2018, doi: 10.31142/ijtsrd15928.

[9] R. Srivastava, S. Kumar, and A. S. | H. M. Saraswat, "Blockchain : A Revolutionary Technology," *Int. J. Trend Sci. Res. Dev.*, 2018, doi: 10.31142/ijtsrd12751.

[10] N. Rifi, N. Agoulmine, N. Chendeb Taher, and E. Rachkidi, "Blockchain Technology: Is It a Good Candidate for Securing IoT Sensitive Medical Data?," *Wirel. Commun. Mob. Comput.*, 2018, doi: 10.1155/2018/9763937.