International Journal of Advances in Scientific Research and Engineering (IJASRE)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2023.9.2.6

Volume 9, Issue 2
February - 2023

A Blockchain Applications and Challenges

Amal Abdulbaqi Maryoosh[1], Ahmed Abd Ali Abdulkadhim[1], MuntahaAbdulzahra Hatem[2]

[1]Computer Science Department, Collage of Education, Mustansiriyah University

[2]Mission and Cultural Relations, Ministry of Higher Education and Scientific Research

Baghdad, Iraq

ABSTRACT

Blockchain is a technology for securely storing data in a manner that makes system changes or hacks impossible or difficult. Numerous organizations have adopted this technology, which utilizes a peer-to-peer distributed network. using a decentralized peer-to-peer network to operate. A blockchain is a collection of linked computer systems that operate as a distributed ledger of Cchain is made up of numerous transactions. This paper aims to explain blockchain technology, including its uses and difficulties.

Keywords: Blockchain, Bit coin, Cryptography, Network, Internet of Things.

1. INTRODUCTION

To construct Bitcoin, blockchain technology was developed. Presented to the world in 2008 in a white paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System", written by an author who has never been identified by their real name, Satoshi Nakamoto. Bitcoin's declared purpose was to lower transaction fees, fraud, and payment uncertainty in online transactions. It was put forth as a substitute for the widely used e-commerce model, which depends on financial institutions acting as trusted third parties to process electronic payments[1].

A blockchain is a series of blocks that functions as a public ledger for all committed transactions. This chain grows when additional blocks are added to it. Decentralization, persistence, anonymity, and audibility are important characteristics of blockchain technology. Blockchain can function in a decentralized setting by fusing important technologies like cryptographic hash, digital signature (based on asymmetric cryptography), and distributed consensus process. Using blockchain technology, a transaction can be carried out independently. Blockchain can significantly reduce expenses and increase efficiency as a result[2].

As opposed to a conventional database, which is controlled by a single entity like banks or governments, A Blockchain is not someone's property. With a vast network watching over it, it becomes nearly hard to tamper with the system by fabricating documents, transactions, and other information. Blockchain is a network of nodes that stores data forever. By doing this, the information is distributed as well as decentralized (Figure 1). A localized version of the Blockchain technology that is updated on a regular basis to maintain consistency across all nodes, can be stored locally by each node in the networkAblockchain is a platform for decentralized computing and information exchange that enables numerous nodes, who do not trust one another, to participate in decision-making. The single point of failure in a centralized system is the issue. A decentralized system avoids having a single point of failure by having numerous coordinate points. Each node works together to complete the task in a distributed setting. A node connected in a distributed manner is used to represent each user. A replica of the regularly updated Blockchainlist, is kept on file by each node. A node can carry out a variety of tasks, including mining, transaction validation, and transaction initiation[3].

In this paper, we will spotlight about the applications of the blockchain technology and the challenges which faces this technology. The remaining sections in this paper are as follow:

Section two explains how the blockchain works. In section three we show the types of block chain networks. Section four displays the applications of blockchain technology. In section five we explain the most important challenges that facing blockchain technology.

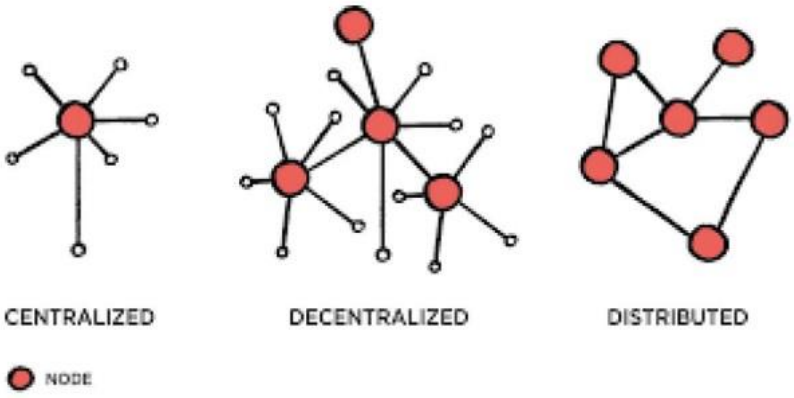

Figure 1: Blockchain as distributed Technology[4].

2. HOW DOES BLOCKCHAIN WORKS?

A node in a network notifies all other nodes of a transaction whenever it gives money to or receives money from another node. In essence, the information indicates that payment of value X was made from node A to node B at a particular moment. A third node, known as a miner, checks the legitimacy of the transaction before registering it in the distributed ledger. A large number of transactions are registered at once in blocks. A new block must be connected to the earlier blocks in some way because these blocks of transactions can be produced by many nodes in the network.Each new block in a blockchain is "chained" to the older blocks by means of a cryptographic signature. While very difficult to duplicate, this signature is simple to validate. It is produced by the cryptographic process known as hashing, which uses a significant amount of information as input to produce a special identification known as the "hash value" or "digital fingerprint." It is difficult to reconstruct the data that produced the hash value via hashing. Miners are nodes that create new block[1], [5].

In the Bitcoin network, a consensus method known as proof of work (POW) is employed. For authentication, POW needs a challenging computing procedure. In POW, each node in the network computes a hash value of the block header, which is continually updating. According to the consensus, the estimated value must be less than or equal to a specific given value. To reach the aim in the decentralized network, all members must continuously calculate the hash value using various nonces. All other nodes must mutually verify the accuracy of the value when one node obtains the pertinent value. Then, in the event of fraud, the transactions in the new block would be verified. Then, a new block is added to the blockchain to represent the authenticated result, which was determined from the collection of transactions utilized for the calculations.The POW mechanism is known as mining, and the nodes that calculate the hashes are known as miners. An incentive mechanism (such as giving the miner a small share of Bitcoins) is also suggested because calculating the authentication is a time-consuming procedure[2].The Sybil or 51 percent assault, which happens when a malicious actor controls a majority of the nodes and then decides to reach a consensus against the interests of other network users, is one of the risks to the blockchain.[1].

DOI: 10.31695/IJASRE.2023.9.2.6

3. TYPES OF BLOCKCHAIN NETWORKS

A Blockchain depending on its applications can be classified into public, private, or hybrid[6], [7]as shown in Figure 2.

a. **Public block chain: It** is a fully decentralized network, it has no single owner, is permission less, visible by anyone, and with no individual or entity controlling it. All transactions are fully decentralized and transparent by allowing anyone to participate. Bitcoin is an example of a public blockchain.

b. **Private block chain:** A private blockchain (also called permissioned) is distinguished from a public blockchain in that it is centralized participants are required to ask for consent to join the network. Only the entity inside the network will gain permission to write to and read from the blockchain. Because a single entity owns and controls the creation of blocks, consensus procedures and mining are typically not necessary.

c. **Hybrid block chain:** The hybrid blockchain, also known as consortiums, has some features of the private blockchain, such as scalability, security, and privacy protection level. The main difference is that type nodes, such as the leader node, are selected to verify transactions instead of a single entity. Only authorized members are given copies of the blockchain, making the network partially decentralized.

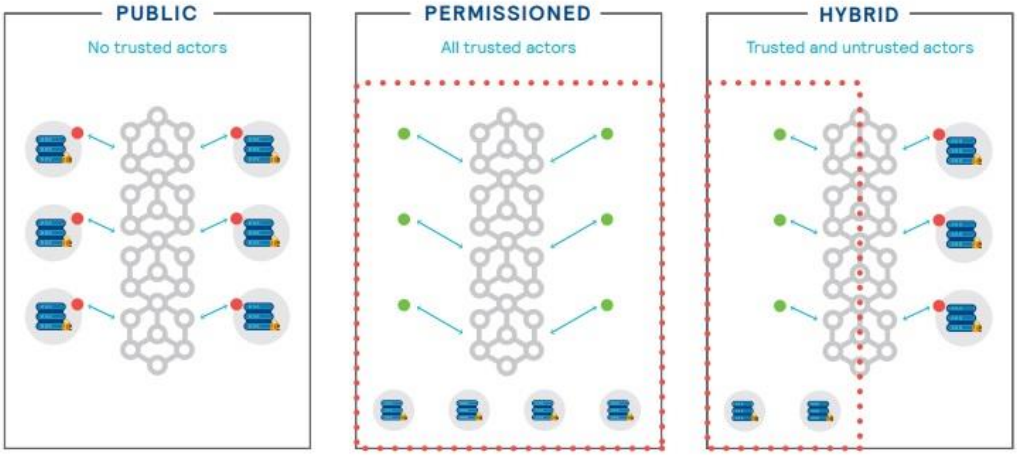

Figure 2: Types of Blockchain Networks[8]

4. APPLICATIONS OF BLOCKCHAIN

The applications of the blockchain have expanded to include many areas while it was in its infancy an application for cryptocurrencies. As its uses have expanded to include many areas such as supply chain management, internet of things,energy-saving, advertising verification, healthcare, and etc... With the creation of user-friendly interfaces and new use cases, it is anticipated that we will see applications that are more beneficial in the future. Businesses and sectors are motivated to explore and build blockchain-based applications for a variety of reasons, including access to information, data integrity, and operational resilience[9].

4.1. Financial Applications

One of the biggest challenges of the financial industry is the centralization of financial institutions. This contradicts the special feature of Blockchain technology. However, recent development in the type of technology has addressed this problem. Another challenge is the transaction per second of the financial institution. Aside from that, cost initiation, implementation, and maintenance are of major concern. These require a great amount of funding to initialize and implement because the whole system includes the hardware and software. Moreover, financial institutions require large-scale integration and migration from the previous system and maintenance of the whole system. Implementing this might be a big issue for a small financial institution. It

DOI: 10.31695/IJASRE.2023.9.2.6

also requires expert personnel to implement, maintain and operate the system, since Blockchain is still under development as a whole, technical training is not yet in-depth across the network and its application[7].

4.2. Internet of Things

The using of Blockchain technology with Internet of Things (IoT) can enhance security and privacy. Blockchain eliminates the idea of centralized IoT and allows for the secure and efficient transfer of data for every transaction. With the aid of blockchain-IoT integration, a number of important applications for smart environments were created. These apps' prototypes must be studied in order to identify and address their flaws.Here, we list few Blockchain technology applications forIoT[4], [9], [10]:

1- Energy Trading.

2- Internet of Vehicles.

3- Internet of Healthcare things.

4- The cloud as a potential platform.

5- Implementations in a smart city network.

6- Applications in Industrial Internet of Things.

4.3. Healthcare Applications

When using Blockchain technology in Electronic Medical Records (EMRs), EMRs are current and offer secure, private sharing of patient data among numerous providers. Blockchain technology in healthcare has benefits beyond security and privacy. Regardless of their electronic medical systems, doctors, hospitals, patients, and all other stakeholders might access a shared database of health data and information on the blockchain. Its use frees up more time for doctors to care for patients and share more research findings that could lead to the development of new therapies. By making results more available and reducing claim and billing fraud, it helps improve medication development. Blockchain is transforming how the healthcare sector runs[7], [9].

4.4. Smart Contracts

When implemented on the blockchain, a smart contract is a computer system or collection of code and data that executes automatically based on predetermined criteria[11]. Without the use of middlemen, smart contracts offer the chance to exchange money, shares, properties, and other assets directly. Users of the Ethereum network can develop "smart contracts." Any machine with the Ethereum software installed can be used for this[12]. Smart contracts can be used to detect and stop malicious behavior. The system rejects the device's breached blockchain updates. In cases where devices don't require centralized devices for secure communication, they also get rid of centralized organizations. Instead, with the aid of smart contracts, they may safely connect with one another, share data, and carry out operations autonomously[13].

4.5. Education System

There are various issues that arise in this day and age when school instruction is delivered online. Classes are condensed, and the teacher must continuously check to see who is in the class, taking up valuable time. Each school's administrator is also interested in finding out if the staff teachers hold their classes consistently and on schedule. If the data from each class were stored on a blockchain, these issues might be solved. No one will be able to modify the data that way. You can always find out who taught the class, when they taught it, and who showed up. Students would attend lessons more frequently if they were aware that everything was recorded and that the information was unchangeable. And it is an essential requirement if they want to increase their success. For instructors, the biggest satisfaction comes from increased student achievement. Parents would likewise be happier if their kids behaved in this way. A good education would be most advantageous to society as a whole because knowledge

DOI: 10.31695/IJASRE.2023.9.2.6

is power. And it is an essential requirement if they want to increase their success. For instructors, the biggest satisfaction comes from increased student achievement. Parents would likewise be happier if their kids behaved in this way. A good education would be most advantageous to society as a whole because knowledge is power[11].

5. CHALLENGES OF BLOCKCHAIN

The blockchain has a lot of potential, but it also has a lot of problems that prevent it from being widely used. In this section, we will discuss the most important current challenges facing blockchain technology.

5.1. Privacy

Blockchain can preserve a certain amount of privacy and security of data processing, however, it is cannot guarantee transactional privacy because collected data are publicly visible and available for all readers. According to a recent study, it is possible to link a user's Bitcoin transactions and learn personal information about them. Furthermore, open ledgers could cause privacy problems because IoT ubiquitous sensing technologies continuously capture sensitive and personal data from customers [14], [15]. Data privacy could be secured with private blockchain ledgers by enabling encryption and granting restricted access to the ledgers. However, these private blockchain systems will restrict how much of the vast amounts of data that AI may need to digest and carry out accurate and correct decision-making and analytics may be accessed and exposed[15].

5.2. Scalability

One of the main issues with the blockchain platform of today is its scalability. The blockchain grows in size as more transactions are made every day. Since they must determine if the source of the current transaction is unspent or not, each node must store all transactions in order to validate them. Additionally, the Bitcoinblockchain can only process about 7 transactions per second due to the original restriction on block size and the time interval used to generate a new block; this performance is really unacceptable when compared to Facebook, which processes millions of transactions every second, including likes, posts, and comments. Since the capacity of blocks is so low, many minor transactions may be delayed since miners prioritize those with significant fee income. Several initiatives have been put out to remedy the blockchain's scalability issue, such as storage optimization of blockchain and redesigning blockchain[14-15].

5.3. Security

Blockchain technology's decentralized power is subject to exploitation and misuse. The blockchain systems are susceptible to cyberattacks like that 51% attack, despite the fact that blockchain offers strong methods for safeguarding IoT and predictive analyses. In public blockchains like Ethereum and bitcoin, this security issue is more obvious. Because consensus methods are specified among parties, private blockchain platforms are less affected by this issue. Additionally, the mining nodes' operating environment is not secure, particularly on private blockchain platforms like Hyperledger with a small number of mining nodes, where the results of the execution might be changed. Newly emerging blockchain technologies, such Intel SGX, are outfitted with hardware to provide execution in a Trusted Execution Environment to address this issue[15].

6. CONCLUSION

Blockchain is a peer-to-peer, decentralized digital ledger that is accessible to the public. Numerous applications of blockchain allow transactions to be carried out in a secure setting without the involvement of a third party. Blockchain technology has the potential to transform the current centralized system into a decentralized one from the perspective of applications. The Internet of Things (IoT), healthcare, and other application areas have been listed as some of the most demanding. Blockchain technology has many benefits, including decentralization, transparent transactions, openness, and security. However, more study needs to be done on the blockchain system's network, scalability, and mining process.

DOI: 10.31695/IJASRE.2023.9.2.6

REFERENCES

[1] U. Nations, *Harnessing blockchain for sustainable development*. 2021. doi: 10.18356/9789214030430c007.

[2] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities : A Survey Shaoan Xie Hong-Ning Dai Huaimin Wang," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 1–24, 2017, [Online]. Available: http://inpluslab.sysu.edu.cn/files/blockchain/blockchain.pdf

[3] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy Challenges," *Internet of Things (Netherlands)*, vol. 8, p. 100107, 2019, doi: 10.1016/j.iot.2019.100107.

[4] P. Ahmad, "A Review on Blockchain's Applications and Implementations," *ADCAIJ Adv. Distrib. Comput. Artif. Intell. J.*, vol. 10, no. 2, pp. 197–208, 2021, doi: 10.14201/adcaij2021102197208.

[5] A. Lewis, "Blockchain Technology Explained," *Blockchain Technol.*, pp. 1–27, 2015, [Online]. Available: http://www.blockchaintechnologies.com/blockchain-definition

[6] K. Sultan, U. Ruhi, and R. Lakhani, "Conceptualizing blockchains: Characteristics & applications," *Proc. 11th IADIS Int. Conf. Inf. Syst. 2018, IS 2018*, pp. 49–57, 2018.

[7] N. E. Villanueva, "Blockchain Technology Application: Challenges, Limitations and Issues," *J. Comput. Innov. Eng. Appl.*, vol. 5, no. 2, pp. 8–14, 2021.

[8] P. Fuch, "B lo c kc h a i n," 2019, [Online]. Available: https://www.mercer.com/content/dam/mercer/attachments/private/gl-2019-blockchain-101-overview-mercer.pdf

[9] W. Baiod, J. Light, and A. Mahanti, "Blockchain Technology and its Applications Across Multiple Domains: A Survey," *J. Int. Technol. Inf. Manag.*, vol. 29, no. 4, pp. 78–119, 2021, [Online]. Available: https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1482&context=jitim

[10] M. Ebrahim, A. Hafid, and E. Elie, "Blockchain as privacy and security solution for smart environments: A Survey," vol. 1, 2022, [Online]. Available: http://arxiv.org/abs/2203.08901

[11] M. Mijoska and B. Ristevski, "Possibilities for applying blockchain technology – A survey," *Inform.*, vol. 45, no. 3, pp. 319–333, 2021, doi: 10.31449/INF.V45I3.3248.

[12] I. K. Utakaeva, "Directions and features of application of the blockchain technology," *J. Phys. Conf. Ser.*, vol. 1353, no. 1, 2019, doi: 10.1088/1742-6596/1353/1/012103.

[13] N. Tariq *et al.*, "The security of big data in fog-enabled iot applications including blockchain: A survey," *Sensors (Switzerland)*, vol. 19, no. 8, pp. 1–33, 2019, doi: 10.3390/s19081788.

[14] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, no. c, pp. 10127–10149, 2019, doi: 10.1109/ACCESS.2018.2890507.

[15] Z. A. Shao Qifeng, Jin Cheqing, Zhang Zhao, Qian Weining, "Blockchain technology: architecture and progress," 计算机学报, no. 4, pp. 1264–1268, 2018.

DOI: 10.31695/IJASRE.2023.9.2.6