Metaverse Basic and Applied Research. 2022; 1:18
doi: 10.56294/mr202218

SHORT COMMUNICATION

Understanding Blockchain Technology: How It Works and What It Can Do

Comprendiendo la tecnología blockchain: Cómo funciona y lo que puede hacer

Barnali Gupta[1]

[1]International Institute of Information Technology, Center for Security, Theory and Algorithmic Research. Hyderabad, India.

Cite as: Gupta B. Understanding Blockchain Technology: How It Works and What It Can Do. Metaverse Basic and Applied Research. 2022; 1:18. https://doi.org/10.56294/mr202218

Submitted: 01-11-2023 **Revised:** 20-11-2022 **Accepted:** 27-12-2022 **Published:** 28-12-2022

Editor: Dra. Patricia Alonso Galbán

ABSTRACT

Blockchain is a chain of blocks that are connected together and are continuously growing by storing transactions on the blocks. This platform uses a decentralized approach that allows the information to be distributed and that each piece of distributed information or commonly known as data have shared ownership. Blockchains holds batches of transactions that are hashed thus providing them security and they are managed by peer-to-peer networks. Blockchain, an information administration method, has the potential to encourage responsibility and openness. In a blockchain, each user of the computer network can access the same copy of the transaction ledger. The blockchain technology has the potential to handle various security attacks as it can eliminate the need of the centralized authority to perform various operations. In the blockchain technology, a number of users participate in transaction verification and validation.

Keywords: Blockchain; Distributed Information; Information Administration; Open Blockchain; Individual Blockchain; Hybrid Blockchain; Consortium Blockchain.

RESUMEN

Blockchain es una cadena de bloques que están conectados y en constante crecimiento mediante el almacenamiento de transacciones en los bloques. Esta plataforma utiliza un enfoque descentralizado que permite que la información sea distribuida y que cada pieza de información distribuida, comúnmente conocida como datos, tenga una propiedad compartida. Los bloques de la cadena de bloques contienen lotes de transacciones que están cifrados, lo que les proporciona seguridad y son gestionados por redes peer-to-peer. Blockchain, un método de administración de información, tiene el potencial de fomentar la responsabilidad y la transparencia. En un blockchain, cada usuario de la red informática puede acceder a la misma copia del libro mayor de transacciones. La tecnología blockchain tiene el potencial de manejar varios ataques de seguridad, ya que puede eliminar la necesidad de una autoridad centralizada para realizar diversas operaciones. En la tecnología blockchain, varios usuarios participan en la verificación y validación de las transacciones.

Palabras clave: Blockchain; Información Distribuida; Administración de Información; Open Blockchain; Blockchain Individual; Blockchain Híbrido; Blockchain Consorcio.

INTRODUCTION

Blockchain is a chain of blocks that are connected together and are continuously growing by storing transactions on the blocks. This platform uses a decentralized approach that allows the information to be distributed and that each piece of distributed information or commonly known as data have shared ownership.

Blockchains holds batches of transactions that are hashed thus providing them security and they are managed by peer-to-peer networks.[1]

A blockchain has certain benefits such as security, anonymity, and integrity of data with no third-party intervention. These benefits make it a reasonable choice to store patient's medical records on it, because the innovation of technology in the healthcare industry has made the security of patient's medical data a top priority. A number of researchers have also identified that using blockchain technology in healthcare would be a feasible solution.[1]

The blockchain technology has the potential to handle various security attacks as it can eliminate the need of the centralized authority to perform various operations. In the blockchain technology, a number of users participate in transaction verification and validation.[2]

The blockchain reduces the risk of single point of failure and network attacks using the distributed network nodes. Use of the decentralized platform reduces fraud by time stamping entries, and information of users is stored in immutable ledger across the network using the smart contact. Blockchain eliminates manual processes like reconciliation between multiple isolated ledger and administrative processes which helps to reduce the cost of the system. Due to the use of various cryptographic linked chains, the speed of transaction and level of security is enhanced manyfold.[2]

DEVELOPMENT

Blockchain

Blockchain, an information administration method, has the potential to encourage responsibility and openness. In a blockchain, each user of the computer network can access the same copy of the transaction ledger. Data entered into the system cannot be changed afterward, and before it is added to the ledger, it is verified by other network users. Blockchain was primarily designed for cryptocurrencies in order to do away with the necessity for middlemen like banks and to guard against a high risk of fraud and theft.[3]

Key Characteristics

Below are some key characteristics of block chain:[4]

- Data Immutability: this is the most important aspect since it guarantees that no data will be damaged. Every node in the system has a copy of the ledger, which is how this works. Therefore, every node must agree in order to change any data. Blockchain is now transparent and safe.
- Decentralized: Blockchain technology is decentralized, which means it is not controlled by a single person, a single authority or government. Instead, a number of nodes oversee the entire process.
- A single trustworthy source: in a blockchain, the distributed ledger serves as the lone source of truth. As a consequence, if you want to look up a certain transaction or discover who owns something, you just need to visit one place.
- Provenance: with blockchain, every transaction, whether physical or digital, can be tracked from beginning to end.
- Algorithm: all parties or nodes must concur to abide by the same rules for a transaction to be approved and recorded on the blockchain.
- Anonymous: although each transaction is open to the public and transparent, the addresses serve to conceal the identities of the parties involved. For instance, in the case of a money transfer, the recipient will only be aware of the fact that the sender is associated with a bitcoin address but not the address itself. One of the many explanations for this is privacy.

Figure 1 shows the working steps of a Blockchain.

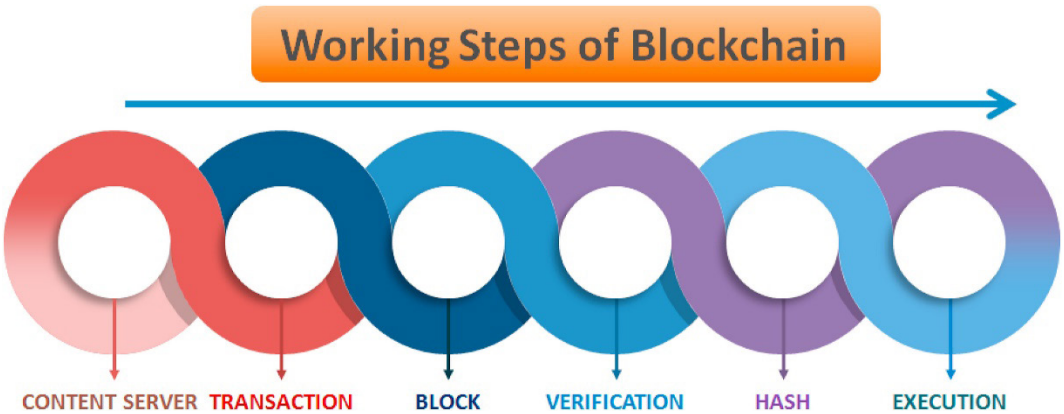

Figure 1. Working steps of a Blockchain

https://doi.org/10.56294/mr202218

Types of block chain

Open Blockchain

The decentralized systems principle can be fully implemented on these blockchains. There are no restrictions; anybody with a computer and internet access is welcome to join the network.[5] Because of its public moniker, which suggests that it is not under the authority of any one party, this blockchain is available to all users. Anyone who has internet connection and a computer with dependable hardware is eligible to participate in this open blockchain. Any additional nodes or network blocks that are there are copies on each machine in the network. On this public blockchain technology, we may also do transactions or document validation.

- Advantages:
  1. Reliable: There are algorithms that spot any fraud. Participants don't need to be concerned about the network's other nodes.
  2. Secure: This type of blockchain is significant since everyone may use it. A wider variety of records are available in a sizable size.
- Disadvantages:
  1. Processing: Due to the transaction's size, the process goes very slowly. It takes a long time to validate every node.
  2. Power Consumption: It takes a lot of energy to create proof of work. A high-quality computer system is necessary in order to join the network.
  3. Recognition: Since there is no centralized authority, governments must cope with the difficulty of deploying technology more swiftly.

Individual Blockchain

These digital currencies are not as randomized as the public blockchain technology, which is the most secure of the bunch because only a select few nodes are allowed to participate.[6] These are opaquer than an open network. They are accessible only to specific permitted individuals. These distributed ledgers function on a private network. In this, an intranet within a company or organization is solely accessible to a small number of people.

- Advantages:
  1. Speed: The rate is high because the transaction is so little. Verification of each node requires less time.
  2. Scalability: The scaling parameters are modifiable. The network's size can be manually selected.
  3. Privacy: The degree of privacy has increased as a result of business demands for concealment.
- Disadvantages:
  1. Security: Since there aren't as many nodes of this kind, there's a chance that someone may control them. There are more security dangers with these blockchains.
  2. The difficulty of building confidence is one of its main problems as a result of bureaucracy. Companies may use this technique to punish wrongdoing.
  3. The distributed ledger system in its entirety might be in jeopardy if any of the nodes fall due to a limited amount available node.

Hybrid Blockchain

It is made up of a combination of public as well as private blockchain content, some of which is controlled by a particular organization and some of which is made available to the public.[7] It combines blockchains that are both public and private. Both permissioned and non-permissioned systems are used. Smart contracts make it possible for consumers to get information. Although a major entity is the legitimate proprietor of the combined blockchain, it cannot alter a transaction.

- Advantages:
  1. Ecosystem: The main advantage of this cryptocurrency is that it is hybrid. It cannot be hacked since 51 % of users do not have access to the network.
  2. Price: Transfers are cheap since just a small number of nodes validate them. There is a decrease in the computational expense since not all nodes do the verification.
- Disadvantages:
  1. Efficacy: A hybrid Bitcoin is not accessible to everyone. Additionally, the company has certain issues with maintenance efficacy.
  2. Slide: the individual may be given the option to have some information hidden. Whether an individual who requests access via a type of hybrid blockchain would be granted it depends upon the organization.

https://doi.org/10.56294/mr202218

Consortium Blockchain

It is a novel approach that satisfies the needs of the organization. This blockchain, which also transmits or receives transactions, validates the transaction. Another term for it is Federal Blockchain.[8] This strategy is new in how it responds to the needs of the company, there are public and private areas and the blockchain is controlled by several entities under this system.

- Advantages:
  1. Quickness: Because there aren't many users, verification happens quickly. The quick pace may make this more appealing to businesses.
  2. Authority: It might involve several institutions and be distributed at every level. Power that is not centralized improves security.
- Disadvantages:
  1. Approval: Because the process has the backing of all the members, it is less pliable. Since multiple entities are involved, there may be differences in the vision of interest.
  2. Openness: The organization might be attacked if it becomes corrupt. Organizations may hide data from users.

Consequences Mechanism

Evidence of work

The nodes participate in mineral extraction, which is a different name for the Proof of Work (POW) procedure. The difficult problems in mathematics that miners solve require a lot of computing power. ASIC mining, mining pools, CPU mineral extraction, GPU mineral extraction, FPGA mineral extraction, and many more methods of mining are used by miners to accomplish this. A block is awarded to a miner if they are the first to solve a mathematical puzzle. Trial and error are the only method to get the issues resolved. As a result of this, miners require a growing amount of computing processing power in order to get evidence of ownership.[9,10]

Evidence of ownership

Confirmation of Interest (POS) uses a random technique to decide who gets a chance to build the next block. Users of Blockchain can lock up the tokens they own by being validators for a predetermined amount of time. When a user reaches the validator status, they can build blocks. Validation can also be selected based on the architecture of the blockchain. Generally speaking, the possibility of building a new block is higher for the individual with the highest stake or longer ownership of the currency.[11,12]

Evidence of captivity

The proving of Capability method is putting solutions to challenging mathematical puzzles on digital storage devices like hard drives. The whole procedure of accomplishing this is plotting. Once a storage device has been filled with the solutions to mathematical issues, users can utilize it to manufacture blocks. The ability to develop new blocks is provided to users that resolve the issues the fastest. As a result, people with more storage will be more likely to generate new blocks.[13,14]

Evidence of ethnicity

In Evidence of the concept of identity, a user's private key is contrasted with an approved identity. A Proof of Identity is essentially a cryptography document that connects a user's private key to a specific transaction. Any registered user on a distributed ledger system can create a block of data which will be visible to everyone else on the network as a whole. Proof of identification ensures accuracy of information or integrity. Additionally, Proof of Identity, a blockchain consensus method, may be used by smart cities to validate resident citizenship.[15,16,17]

Figure 1 summarize some of the potential uses of block chain in health domain, such as:

1. Blockchain works best for transactions that leave just an unimportant alphanumeric trace and profit from photograph and fixity. Block chain may be chiefly helpful in the healthcare industry for handling dynamic patient consent, data sharing and access permissions, medical and pharmaceutical supply chain management, and identity verification.[18,19,20]
2. Blockchain-enabled solutions are emerging to combat the COVID-19 pandemic, this as an authentication system to facilitate contact tracing in South Korea and a system to support swapping information and software code for research. Additionally, handling of the supply chain for medicines, medical equipment, and prospective vaccinations has been suggested or used with blockchain.[21]
3. For particular deals in the healthcare industry, such as those involving the purchasing along with shipment of drugs and medical supplies chains of custody, as well as the oversight of staff using places of confinement, records pertaining to patients, and other kinds of medical data, complete and permanent keeping of records may be essential.[22,23,24]

4. The rate of advancement in the field of healthcare is accelerating at ever-increasing rates. Presently, there is a demand for high-quality medical facilities that are backed by cutting-edge and modern technology. Here, Blockchain would be important in revolutionizing the healthcare industry. Additionally, the structure of the healthcare system is changing in favor of a patient-centered strategy that emphasises two key components: always having access to the right resources for treatment. Healthcare firms may better deliver proper patient care and top-notch medical facilities thanks to the blockchain. Using this technology, the time-consuming, repeated process of health information exchange, which contributes to high healthcare expenses, may be resolved swiftly. Citizens can participate in health research programs using Blockchain technology.[25,26]

Figure 2. Potential of blockchain in health care

REFERENCES

1. Shahnaz A, Qamar U, Khalid A. Using Blockchain for Electronic Health Records. IEEE Access 2019;7:147782–95. https://doi.org/10.1109/ACCESS.2019.2946373.

2. Bodkhe U, Tanwar S, Parekh K, Khanpara P, Tyagi S, Kumar N, et al. Blockchain for Industry 4.0: A Comprehensive Review. IEEE Access 2020;8:79764–800. https://doi.org/10.1109/ACCESS.2020.2988579.

3. Yang Q, Zhao Y, Huang H, Xiong Z, Kang J, Zheng Z. Fusing Blockchain and AI With Metaverse: A Survey. IEEE Open Journal of the Computer Society 2022;3:122–36. https://doi.org/10.1109/OJCS.2022.3188249.

4. Singh S, Hosen ASMS, Yoon B. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. IEEE Access 2021;9:13938–59. https://doi.org/10.1109/ACCESS.2021.3051602.

5. Nofer M, Gomber P, Hinz O, Schiereck D. Blockchain. Bus Inf Syst Eng 2017;59:183–7. https://doi.org/10.1007/s12599-017-0467-3.

6. Frizzo-Barker J, Chow-White PA, Adams PR, Mentanko J, Ha D, Green S. Blockchain as a disruptive technology for business: A systematic review. International Journal of Information Management 2020;51:102029. https://doi.org/10.1016/j.ijinfomgt.2019.10.014.

7. Centobelli P, Cerchione R, Vecchio PD, Oropallo E, Secundo G. Blockchain technology for bridging trust, traceability and transparency in circular supply chain. Information & Management 2022;59:103508. https://doi.org/10.1016/j.im.2021.103508.

8. Dib O, Brousmiche K-L, Durand A, Thea E, Hamida EB. Consortium blockchains: Overview, applications and challenges. Int J Adv Telecommun 2018;11:51–64.

9. Calvão F. Crypto-miners: Digital labor and the power of blockchain technology. Economic Anthropology 2019;6:123–34. https://doi.org/10.1002/sea2.12136.

10. Kumar A, Kumar Sharma D, Nayyar A, Singh S, Yoon B. Lightweight Proof of Game (LPoG): A Proof of Work (PoW)'s Extended Lightweight Consensus Algorithm for Wearable Kidneys. Sensors 2020;20:2868. https://doi.org/10.3390/s20102868.

11. Bocek T, Stiller B. Smart Contracts – Blockchains in the Wings. In: Linnhoff-Popien C, Schneider R, Zaddach M, editors. Digital Marketplaces Unleashed, Berlin, Heidelberg: Springer; 2018, p. 169–84. https://doi.org/10.1007/978-3-662-49275-8_19.

12. Wang B, Li Z, Li H. Hybrid Consensus Algorithm Based on Modified Proof-of-Probability and DPoS. Future Internet 2020;12:122. https://doi.org/10.3390/fi12080122.

13. Azbeg K, Ouchetto O, Jai Andaloussi S, Fetjah L. An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions. In: Saeed F, Al-Hadhrami T, Mohammed F, Mohammed E, editors. Advances on Smart and Soft Computing, Singapore: Springer; 2021, p. 357–69. https://doi.org/10.1007/978-981-15-6048-4_31.

14. Ray PP, Dash D, Salah K, Kumar N. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. IEEE Systems Journal 2021;15:85–94. https://doi.org/10.1109/JSYST.2020.2963840.

15. Sung CS, Park JY. Understanding of blockchain-based identity management system adoption in the public sector. Journal of Enterprise Information Management 2021;34:1481–505. https://doi.org/10.1108/JEIM-12-2020-0532.

16. Lee J-H. BIDaaS: Blockchain Based ID As a Service. IEEE Access 2018;6:2274–8. https://doi.org/10.1109/ACCESS.2017.2782733.

17. Liu Y, He D, Obaidat MS, Kumar N, Khan MK, Raymond Choo K-K. Blockchain-based identity management systems: A review. Journal of Network and Computer Applications 2020;166:102731. https://doi.org/10.1016/j.jnca.2020.102731.

18. Kaushik A, Choudhary A, Ektare C, Thomas D, Akram S. Blockchain — Literature survey. 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017, p. 2145–8. https://doi.org/10.1109/RTEICT.2017.8256979.

19. Stephen R, Alex A. A Review on BlockChain Security. IOP Conf Ser: Mater Sci Eng 2018;396:012030. https://doi.org/10.1088/1757-899X/396/1/012030.

20. Ahram T, Sargolzaei A, Sargolzaei S, Daniels J, Amaba B. Blockchain technology innovations. 2017 IEEE Technology & Engineering Management Conference (TEMSCON), 2017, p. 137–41. https://doi.org/10.1109/TEMSCON.2017.7998367.

21. Cui Z, XUE F, Zhang S, Cai X, Cao Y, Zhang W, et al. A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. IEEE Transactions on Services Computing 2020;13:241–51. https://doi.org/10.1109/TSC.2020.2964537.

22. Prokofieva M, Miah SJ. Blockchain in healthcare. Australasian Journal of Information Systems 2019;23. https://doi.org/10.3127/ajis.v23i0.2203.

23. Onik MdMH, Aich S, Yang J, Kim C-S, Kim H-C. Chapter 8 - Blockchain in Healthcare: Challenges and Solutions. In: Dey N, Das H, Naik B, Behera HS, editors. Big Data Analytics for Intelligent Healthcare Management, Academic Press; 2019, p. 197–226. https://doi.org/10.1016/B978-0-12-818146-1.00008-8.

24. Mukherjee P, Singh D. The Opportunities of Blockchain in Health 4.0. In: Rosa Righi R da, Alberti AM, Singh M, editors. Blockchain Technology for Industry 4.0: Secure, Decentralized, Distributed and Trusted Industry Environment, Singapore: Springer; 2020, p. 149–64. https://doi.org/10.1007/978-981-15-1137-0_8.

25. Gaynor M, Tuttle-Newhall J, Parker J, Patel A, Tang C. Adoption of Blockchain in Health Care. Journal of Medical Internet Research 2020;22:e17423. https://doi.org/10.2196/17423.

26. El-Gazzar R, Stendal K. Blockchain in Health Care: Hope or Hype? Journal of Medical Internet Research 2020;22:e17199. https://doi.org/10.2196/17199.

FUNDING
No financing.

CONFLICTS OF INTEREST
None.

AUTHOR CONTRIBUTIONS
Conceptualization: Barnali Gupta.
Investigation: Barnali Gupta.
Methodology: Barnali Gupta.
Writing - original draft: Barnali Gupta.
Writing - review and editing: Barnali Gupta.

https://doi.org/10.56294/mr202218