International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN : 2581-9925, Impact Factor: 6.882, Volume 04, No. 03(I), July - September, 2022, pp. 100-104

NEW EDGE IN SECURITY: BLOCKCHAIN

Radhika Sharma*
Amit Garg**

ABSTRACT

Blockchain is a decentralized ledger that records all transactions between peer-to-peer networks. No central authority is needed to confirm transactions using this technology. Blockchain is helpful for all of the following: for business, for technology, and for many other things. Blockchain is a type of next-generation software that can handle tasks in many different realms. Blockchain technology has the ability to decrease the amount of trust needed between corporations and make investments in the technology more financially rewarding. Blockchain is a form of a digital ledger, which records transactions chronologically on a public protocol operating on a distributed network. This paper reviews on the concept of Blockchain, its working principles and also on the applications where the blockchain can be used.

Keywords: *Blockchain Technology, Hashing Algorithms, Security, Next-Generation Software.*

Introduction

Blockchain is a ledger that helps ensures the accuracy of transactions by tracking assets. Anything that can be quantified can be traded on a blockchain network. This reduces risks, since a transaction is recorded transparently. [1]

Blockchain is a ledger with information stored electronically in digital format, which can be shared among nodes on a network. It was originally designed to track transactions between crypto-currencies but has since expanded to tracking all sorts of other transactions. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin. They record all transactions and have security and data fidelity without a need for a third party. [1]

Blockchain technology has a unique structure. Blocks of data are created and stored together in groups to compile a distributed ledger giving the end user access to information about where this information came from. When blocks of data fill up, the old blocks close and are linked together in the chain (known as the Blockchain). Newer blocks that extend after the new block form a new chain. [1]

A database is made of tables and a blockchain forms blocks that form the database. Blockchain inherently has an irreversible timeline. When a block is filled, it's set in stone and becomes a part of this timeline. The timestamp helps us verify that the data is accurate. Each block is added to the chain at a particular time and given an exact timestamp when it is added to the chain. [2]

Components of Blockchain

Blockchain is a ledger used by businesses to track transactions. It can't be changed and is shared by a group in the business network. Blockchain stores records of each transaction or asset transfer, which are verified over time by more blocks created with the same private key. Assets can be anything from intangible items like a patent to a tangible item such as an asset. You can trade these assets on blockchain networks and reduce risk and costs for everyone involved. [3]

Blockchain is a distributed database regularly updated by all the nodes of a computer network. Data is stored in digital format and any new transaction must be validated by other nodes. Blockchains are mostly known for their important role in cryptocurrencies, such as Bitcoin. They maintain a secure record of data and generate trust without the need for an arbitrary third party. [3]

---

* M. Tech Research Scholar, Department of Computer Engineering, Government Women Engineering College, Ajmer, Rajasthan, India.
** Assistant Professor, Department of Computer Engineering, Government Women Engineering College, Ajmer, Rajasthan, India.

Blockchains are mostly known for their important role in cryptocurrencies, such as Bitcoin. They maintain a secure record of data and generate trust without the need for an arbitrary third party. Blockchain data is structured differently than that of a typical database. A blockchain group blocks of information, each containing sets of info. [4]

- **Blocks:** If you accidentally misplace a data file, then all of the data following is scattered. Blockchain technology fixes this problem by linking your lost or changed file to the one following it with a chain.
- **Tables:** A database typically has tables that organize its data, whereas a blockchain is made up of numerous blocks that are strung together. Corporations keep data structured in tables, while blockchain companies choose to structure data in blocks that are joined together. [4]

Corporations keep data structured in tables, while blockchain companies choose to structure data in blocks that are joined together.

The key components in any blockchain ecosystem are as follows:

- **Node Application:** To connect to the blockchain, every computer must have a node app specific to the ecosystem they want to take part in. These include Bitcoin wallet apps and bank chain apps. Participants can come from organizations with a variety of diverse restrictions. For example, Banks are allowed to participate in Bank chain. [5]
- **Distributed Ledger (Database):** Every member in the blockchain ecosystem makes and keeps a copy of the sensitive data. As soon as there is any new update to the ledger, it will be updated for everyone to view. There will be certain guidelines you must follow when running a bitcoin node application. As long as you meet the requirements of the node application, you can enter more than one node application. [5]
- **Consensus Algorithm:** The consensus algorithm provides permanence and security to the data in the blockchain. It shows how the nodes in the network decide what transactions to accept by showing the status of the network. The blockchain can be tampered with by changing the previous block, because it will affect all the blocks after it. It is to be noted that every block in the blockchain contains a hash of its predecessor block. In this way, you have a chain of blocks with enormous work contained. [6]

Blockchain and Security

Blockchain security uses assurance services and frameworks to mitigate fraud. It also has a best practices strategy to protect against cyberattacks. With blockchain, data is encrypted and decentralized. Blockchain technology is resilient to hacking or data alteration.

Every block of information in the chain is connected to all other blocks, making it nearly impossible to tamper with the data. Transactions are authenticated by consensus - a group of authorized users who agree that no content can be changed. There is no single point of failure, and this will ensure transactions cannot be tampered with. [7]

- **Private Blockchains:** To get access to a private blockchain network, one must either be validated by the central administrator or starter. Access can also be granted by settings put in place by the network's administrators. Proof-of-authority is one of the three main consensus mechanisms. It is often used in private blockchains for tasks such as authentication and record keeping. These blockchains keep a customer’s transaction data private.
- **Public Blockchains:** Public blockchains focus on participation and transparency. These transactions can be validated by anyone, and the software code is open-source so the public can view it (e.g., Bitcoin and Ethereum). Public blockchain networks decentralize cooperation throughout a distributed network. The lack of a centralized center of control in public blockchains enables it to operate without central point-of-failure and architectures. The degree of decentralization depends on the design of the consensus algorithm, governance model, and incentive mechanisms. [7]
- **Consortium Blockchains:** When discussing blockchains, public and private are the ones usually talked about but there is a third option: consortium. Consortium blockchains consist of known participants preapproved by a central authority that permits them to participate in the consensus within a network. The semi-permissioned model allows for network decentralization, yet still preserving some control. The private transaction data enabled by this kind of blockchain is what makes it attractive to governments, who are wary of transparency. Consortium

blockchains can reach consensus with “Proof-of-Work” (PoW), “Proof of Authority (PoA) or “Proof-of-Stake” (PoS). There are also others such as delegated proof-of-stake. [7] Consortium blockchains are ideal for use in scenarios where companies are sharing information between themselves or there is a need for a supply chain management.

Applications of Blockchain

Blockchain now has applications in every sector, some of the important sectors are discussed below:

- **Banking and Financial Sector**

The original idea behind the invention of blockchain is still a great application. Blockchain can make online money transfers less expensive and faster than using existing services. Cross-border transactions, even in the U.S., are often slow and expensive. A blockchain transaction can take minutes compared to days for a money transfer between accounts.

Research Work Done in Blockchain in Banking and Financial Sector

J. Han, 2021, The management accounting system of commercial banks is an effective tool for commercial banks. With the help of blockchain technology, commercial banks can build a better data management system and performance evaluation system to increase their core competitiveness. This paper focuses on accounting systems designed for commercial banks. It lays out a possible design, which could optimize data management by integrating AI into the system. [8]

Y. Wang and C. Lin, 2020, This paper aims to explore and solve the difficult problems faced in the development of traditional credit banks, when blockchain technology can be applied to credit banks. The credit chain was designed with Beihang Chain as a prototype, and improved the transaction speed and scalability through new technologies such as domain indexing, concurrency and Byzantine protocol. These innovations can be applied to the construction of a credit bank to provide an effective solution. [9]

N. A. Popova and N. G. Butakova, 2019, Blockchain technology is used to protect information on banking transactions. This is relevant because digital economies are becoming such a large part of today's society. This article details how distributed databases are vulnerable to information theft. It then mentions how blockchain, without tokens, can solve the issue. [10]

- **Insurance**

Blockchain technology helps everyone involved in a transaction find credibility due to the security and transparency it provides. Recording all claims on a blockchain would prevent customers from being able to make duplicate claims for the same event, as well as speeding up the process for claimants that have been compensated.

Research Work Done in Blockchain in Insurance Sector

P. Purswani,2021 the intelligent systems for technologies like IoT and API's are necessary in today's data driven world. Instrumental to increase trust in current and emerging systems, distributed ledgers give up-to-date information that can't be tampered with by users. Parametric insurance can still function without these advances but centralized databases lack transparency for trust issues. This paper deep dives into the technical solution, design challenges, and deployment problems in providing health insurance. The blueprint is an example created for health-based parametric insurance and can be applied to other use cases. [11]

J. Li, et al. 2021 Many sellers of insurance have a bad reputation because they will use fraudulent techniques to delay the application of reasonable claims. One solution is to create an alliance with blockchain and deep learning that can deter the occurrence of fraud. This system links in the intelligent, discriminating scenarios related to insurance into the entire insurance system. Insurance companies have limited accuracy rates, but when combined through blockchains, have a high accuracy rate. This improves the user experience and enhances people’s trust in insurance products. [12]

V. Aleksieva et al. 2020, Blockchain can help reduce insurance claims processing time and operational expenses. This paper presents the results of applying public and private Blockchains for enterprise insurance services. It presents the results from an experiment with Hyper Ledger Fabric and Ethereum smart contracts. [13]

- **Real Estate**

To buy real estate, your bank or mortgage lender will require financial information and papers from the seller that confirm you own the house. To transfer ownership of the house to you, you'll also need deed and title papers. Blockchain technology has been found to be a more secure, accessible way of recording and verifying ownership. Transactions will be sped up and costs reduced as a result.

Data Security: Personal Information

The public ledger, a blockchain, is more secure than current systems. It cannot be hacked as easily. Blockchain technology is used to securely protect identifying information while also giving priority access to those who need it.

Research Work Done in Blockchain in Data Security

G. S. Gunanidhi and R. Krishnaveni, 2022, In the healthcare field, data captured from patients has become increasingly important. G. S. Gunanidhi and R. Krishnaveni published an article in 2022 showing how significant this field is and what can be learned from data collected from patients. The privacy of data leads to securing it with greater quality, requiring a best design methodology. In the present scenario, many failed to provide security of data stored in a server that could be accessed by third parties. To improve the data security and privacy, a consortium model called Enhanced Proof of Work (E-PoW) has been proposed as a cooperative consensus blockchain for an IoT based healthcare monitoring system. [14]

Z. Gong-Guo and Z. Wan, 2021, The limited performance and mobility of IoT devices makes it difficult to support traditional centralized security authentication methods in that environment. The article goes on to mention the Authoritative Parity Consensus Protocol (APCP) as a potential solution. The system contains three types of code: Access Code, Device Code and Policy Code. Access Code is the main program for user authentication with a policy strategy. Device Code provides access to URL data from the storage device and Policy Code uses access control strategy for the administrator user. [15]

L. Boheng, 2021, The idea proposed by L. Boheng would place more sensors on the ground to help companies with production and company security, as well as to train AI networks that would help determine potential dangers specific to that enterprise. [16]

X. Yu, et al. 2021, BC-BLPM is a new access control model for MLS environments. BC-BLPM proposes a 'multi-chain' blockchain architecture providing an improved data protection mechanism which divides resources into isolated access domains. The access control policies are set by a smart contract in each access domain, so that outside of the different side chains will each store and maintain integrity of the records. This AI can adapt well to a multi-level security setting and has the potential for application in the future. [17]

- **Voting**

Blockchain technology can be used to vote on everything from president to school board members because anytime a vote is added, it will show up on the chain. When used, blockchain technology can ensure that no person votes twice, only eligible voters are able to cast their vote, and every vote cannot be tampered with. One way to make voting more accessible would be to use your smartphone to cast a vote by pressing a few buttons. The other option would be to use those same mobile devices as scanners at voting sites, significantly lowering the cost of running an election. [18]

- **Medical Sector**

Blockchain can provide accurate and up-to-date medical data to doctors and other medical professionals. This can ensure that patients get the best care possible when they see multiple doctors. With an AI, medical records can be pulled quickly, which could make a treatment timelier. If insurance information is held in the database, doctors can easily verify if someone is covered and what treatments are available. [18]

- **Logistics and Supply Chain Tracking**

Blockchain technology can provide several advantages in logistics and supply chain networks, including the increased ease of communication. As data is stored on the blockchain, it is secure and cannot be altered. This creates a system of trust as logistics and supply chain partners can work together with more confidence that the data provided is true. [18]

Conclusion

Blockchain can provide secure transactions, reduce compliance costs and also speed up data transfer processing. It helps in the verification and traceability of multistep transactions that need verification and traceability. Use of blockchain technology is beneficial because it helps to manage contracts and ensure the origin of a product. All transactions are secured with cryptography, decentralization, and consensus. The report states that the blockchain market is expected to be valued around 20 billion dollars in 2024.

References

1. Xiong xiong and Zhang jinyi "Overview of the application research of blockchain technology in many fields" Journal of Tianjin University (Social Science Edition) vol. 1 pp. 323-369 2018.
2. B Yu J Wright and S Nepal "Establishing Trust in the Internet of Things Ecosystem Using Blockchain" IEEE Cloud Computing vol. 4 pp. 12-23 2018.
3. M Samaniego and R Deters "Blockchain as a Service for IoT" International Conference on Internet of Things vol. 2 pp. 433-436 2017.
4. S Singh and Singh N. Blockchain "Future of financial and cyber security" Contemporary Computing and Informatics vol. 2 pp. 463-467 2016.
5. K Christidis and M Devetsikiotis "Blockchains and smart contracts for the Internet of things" IEEE Access. vol. 4 pp. 2292-2303 2011.
6. Shao Qifeng Jin Cheqing and Zhang Shao "Blockchain technology: architecture and progress" Chinese Journal of Computers vol. 41 pp. 969-988 2018.
7. Qin Wang Xinqi Zhu Yiyang Ni Li Gu and Hongbo Zhu "Blockchain for the IoT and industrial IoT A review" Internet of Things. vol. 10 pp. 11-13 2020.
8. J. Han, "Intelligent Data Management System and Performance Joint Blockchain Model for Commercial Bank Management Accounting," *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2021, pp. 1525-1528.
9. Y. Wang and C. Lin, "Research on the Application of Blockchain in Credit Bank," *2020 International Conference on Information Science and Education (ICISE-IE)*, Sanya, China, 2020, pp. 298-301.
10. N. A. Popova and N. G. Butakova, "Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions," *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Saint Petersburg and Moscow, Russia, 2019, pp. 1764-1768.
11. P. Purswani, "Blockchain-based Parametric Health Insurance," *2021 IEEE Symposium on Industrial Electronics & Applications (ISIEA)*, Langkawi Island, Malaysia, 2021, pp. 1-5.
12. J. Li, Q. Peng, D. Wu, Y. Sun and W. Zhao, "Lightning Insurance: A Fast Claim, High Accuracy Insurance Platform Based on Blockchain Technology and NASNET Algorithm," *2021 International Conference on Artificial Intelligence and Blockchain Technology (AIBT)*, Beijing, China, 2021, pp. 101-108.
13. V. Aleksieva, H. Valchanov and A. Huliyan, "Smart Contracts based on Private and Public Blockchains for the Purpose of Insurance Services," *2020 International Conference Automatics and Informatics (ICAI)*, Varna, Bulgaria, 2020, pp. 1-4.
14. G. S. Gunanidhi and R. Krishnaveni, "Improved Security Blockchain for IoT based Healthcare monitoring system," *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, Coimbatore, India, 2022, pp. 1244-1247.
15. Z. Gong-Guo and Z. Wan, "Blockchain-based IoT security authentication system," *2021 International Conference on Computer, Blockchain and Financial Development (CBFD)*, Nanjing, China, 2021, pp. 415-418.
16. L. Boheng, "Construction Strategy of Enterprise Security Management Blockchain based on Capsule Network and Situation Awareness1," *2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, Penghu, Taiwan, 2021, pp. 1-2
17. X. Yu, Z. Shu, Q. Li and J. Huang, "BC-BLPM: A multi-level security access control model based on blockchain technology," in *China Communications*, vol. 18, no. 2, pp. 110-135, Feb. 2021.
18. Tang ChengJun Cai Guobao Xu Hui Zhao Ruwen and Ye Jun "Blockchain IoT device and wireless access point two-way authentication scheme" Cyberspace security vol. 10 pp. 8-14 2019.

❖◆❖