ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 11, Issue 11, November 2021 SJIF 2021 = 7.492
A peer reviewed journal

BLOCKCHAIN SOLUTIONS FOR BIG DATA AND IOT CHALLENGES

Dr. Shambhu Bhardwaj*

*Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: shambhu.bhardwaj@gmail.com
DOI: 10.5958/2249-7137.2021.02560.X

ABSTRACT

The widespread use of Blockchain technology, as well as the breadth of its applications, has prompted extensive study in a variety of practical and scientific fields. Although still in its early stages of development, the Blockchain is being hailed as a game-changing solution for contemporary technological issues such as decentralization, trust, identification, data ownership, and data-driven choices. Simultaneously, the world is seeing an increase in the amount and variety of digital data produced by both humans and robots. While trying to figure out the best method to store, organize, and analyze large amounts of data, Blockchain technology comes in handy. Its suggested solutions for decentralized private data management, digital property resolution, IoT connectivity, and public sector reforms are all having a big influence on how Big Data will develop. The innovative solutions related with some of the Big Data domains that may be aided by Blockchain technology are presented in this article.

KEYWORDS: *Big Data, Blockchain, Digital Property, Internet of Things, Privacy, Smart Contracts.*

1. INTRODUCTION

Bitcoin's underlying technology, Blockchain, quickly emerged as Satoshi Nakamoto's true discovery, making Bitcoin merely the first of many future Blockchain implementations. Blockchain is a distributed public ledger that records all of the transactions that have ever taken place in the system. It operates on a peer-to-peer (P2P) network, with each complete node storing a copy of the Blockchain ledger. The Blockchain database is not managed by a central authority. This idea of acquiring a database solely amongst the system's real and equal users lays the groundwork for establishing "decentralized trust." A consensus of nodes that agree on the problem is needed for the transactions to be verified and approved. The notion of decentralized trust is diametrically opposed to virtually every system we've developed using a client-server architecture. There is no longer a mediator processing the actions and data since the central authority has been removed from the system. As a consequence, transaction costs are reduced, transactions are non-reversible, and there is no need for confidence in governments or private businesses. Users of the Blockchain don't even have to trust the other party in the transaction with this approach. Only the system and the code should be trusted(1–3).

A blockchain is a database that organizes transactions into blocks. Blockchain ecosystem is illustrated in Fig. 1 below. When a new transaction is generated, the sender broadcasts it to all other nodes in the P2P network. The deal is still in the works and has yet to be confirmed. The nodes verify the transaction and store it in their transactional pools as soon as they get it.

Validating transactions entails performing specified tests on the transaction's structure and activities. Miners are specialized nodes that generate new blocks that include all or part of the available transactions from their transaction pool. The block is then mined, which is a method of determining the proof of work based on variable data from the new block's header. The continuous computation of a cryptographic hash that meets the specified difficulty goal is used to find the proof of work. Mining requires a significant amount of computing power, and miners use specialized mining gear. The miner who discovers a solution to his or her block first wins. His candidate block gets added to the chain as a new block. We can argue that the newest block in the Blockchain includes the most recent transactions since transactions are added to the mining block as they arrive(4–7).

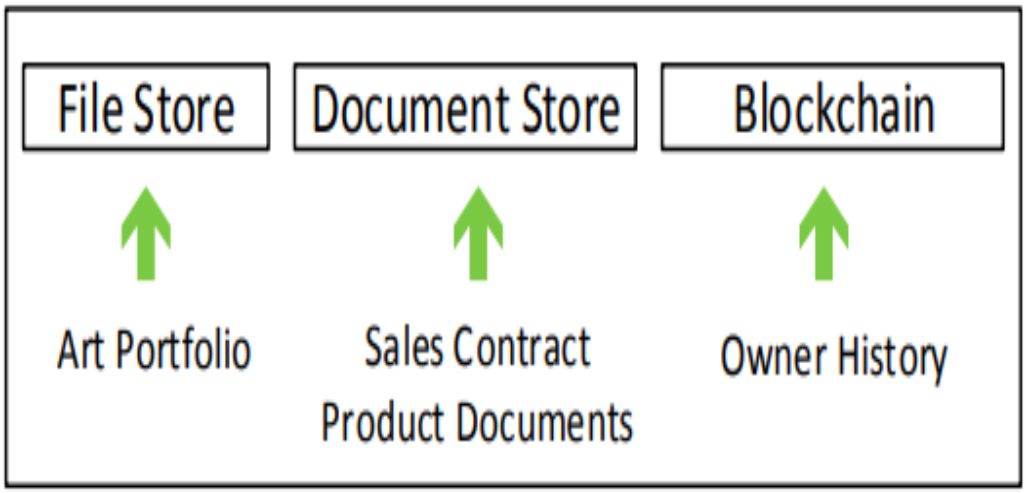

Fig. 1: Blockchain Ecosystem(8)

1.1. Internet of Things (IoT):

The Internet of Things (IoT) is an exciting new idea in development, but there are significant challenges in creating a safe ecosystem that encompasses all components of the IoT architecture. Using current technologies to create IoT systems resulted in a plethora of complicated protocols with contradictory settings. The centralized server-client model is used in today's IoT networks. Through cloud servers, all devices are recognized, authenticated, and linked. The Internet is used to establish a link between devices(7,9–11). Even if this approach works well for the time being, it may not be able to meet the requirements of future IoT ecosystems. Continuing IoT growth in a more decentralized manner was regarded as the right path, but much of the technology, such as privacy and security in large IoT P2P networks, remained lacking. Blockchain technology has the potential to become the perfect component and foundation for monitoring billions of linked devices, processing transactions, and coordinating the devices. Without the need of a centralized cloud, blockchain will enable peer-to-peer communications, file sharing, and autonomous device coordination. According to one IBM study, Blockchain provides the foundation that facilitates device transactions and coordination (12). In the future Internet of Decentralized and Autonomous Things, each item will be in charge of its own function and behavior.

The current state of IoT devices is that they are controlled by the user from a central location. The user's mobile device may serve as the focal point. The user controls all of the activities,

instructions, and rules. While this is beneficial in terms of personal control, it is not fully automated in many respects. If all gadgets are managed by the Blockchain rather than by direct human control, a true revolution may occur. Smart contracts make this feasible. A smart contract is a collection of criteria and business rules that must be fulfilled before a transaction can be recorded on the Blockchain. The transaction recorded on the Blockchain may be more complicated than just transferring ownership. Smart contracts provide a built-in mechanism for carrying out various contract kinds amongst nodes. The smart contract is also self-contained, and theoretically, it is a computer code that can be maintained and performed by itself. When it comes to controlling force, no human element is required. Ethereum, a framework for building Blockchain systems, allows smart contracts to be executed. Ethereum, like Bitcoin, has its own network, nodes, and miners. However, Ethereum nodes are capable of executing any contract that is sent to them.

2. LITERATURE REVIEW

Data is the lifeblood of every company, according to Rabah et al(13). Big data is now used in almost every sector, including retail, healthcare, financial services, government, agriculture, and customer service. Big data may help any company that can use data to solve nagging questions about its operations. Overall, big data is in high demand across all industries and businesses. Those that strive to understand their customers' businesses and issues will be able to discover big data solutions that are suitable for their requirements before their rivals, giving them a competitive edge.

According to Yue et al., the emergence of the big data era on the Internet has resulted in a massive increase in data size(14). However, the most serious problem with big data is a lack of confidence, which makes data safe circulation and industrial growth impossible. By combining non-tampering, traceable characteristics with smart contracts that automatically follow default instructions, blockchain technology offers a novel solution to this issue. They propose a credible large data sharing model based on blockchain technology and smart contracts in their paper, which ensures that data resources are circulated safely.

Internet of Things (IoT) technology, according to Sun et al., has lately grown in popularity(15). However, owing to the limited resources of IoT devices and the centralized system design, several serious problems, such as centralized server overload, single point of failure, and the potential of malicious use of personal information, remain difficult to resolve. In bitcoin trading, blockchain technology has been a huge success. They propose a battery replenishment system for electric vehicles that uses a battery switching method. They also use tests to demonstrate the logic of their approach and compare it to other blockchain-based IoT solutions.

3. DISCUSSION

3.1. Decentralized Protection of Personal Data:

When social media networks gather users' personal data, activities, and habits on a regular basis, they lose control over their privacy. While data-driven services have advantages in terms of customized preferences, consumers still don't have a clear picture of what data is gathered and for what purpose. Users lose all control over what happens to their data after then, and they are unable to revoke authorization. Most social networking platforms include a privacy settings area where users may restrict what other people can view about them. What the social media

company sees is something they can't control or modify. People are used to privacy agreements that are presented in a non-user-friendly manner, outlining just the most basic elements of data collection. However, the collection of personal information does not end when you leave the site. Users' online surfing interests and interactions with other web or mobile apps are tracked by social media platforms. Users' installed mobile applications gather even more personal data, such as contact lists and location. When installing a mobile application, users are forced to simply allow third-party access with no additional information or opportunity for partial approval. Fig. 2 depicts decentralized permissions system.

As we confront the repercussions of what others have seen or learned about us, our concerns about data privacy are growing. In a recent study on the state of privacy conducted in the wake of numerous high-profile data breaches, 74 percent of respondents said it is “very important” to them to have control over who can obtain information about them, and 65 percent said it is “very important” to them to have control over the information collected about them (16). In the same survey, 91 percent of respondents agreed that customers had lost control over how businesses acquire and utilize personal information.

Zyskind et al. offer a method that addresses typical privacy concerns such as data ownership, data openness, auditability, and fine-grained access control(17). This is an access-control management system that focuses mostly on mobile platforms and the user's inability to withdraw authorized access to her personal information. Permissions are given forever when a mobile app is installed, and if the user wishes to withdraw access, she must remove the program and cease using the services. The new solution's aim is to allow users to manage and audit which data is kept and how it is utilized. Access, as previously said, should be revocable. So, the technological concept is to store personal data access rules on the Blockchain and then allow Blockchain nodes to regulate access to a DHT (Distributed Hash Table).

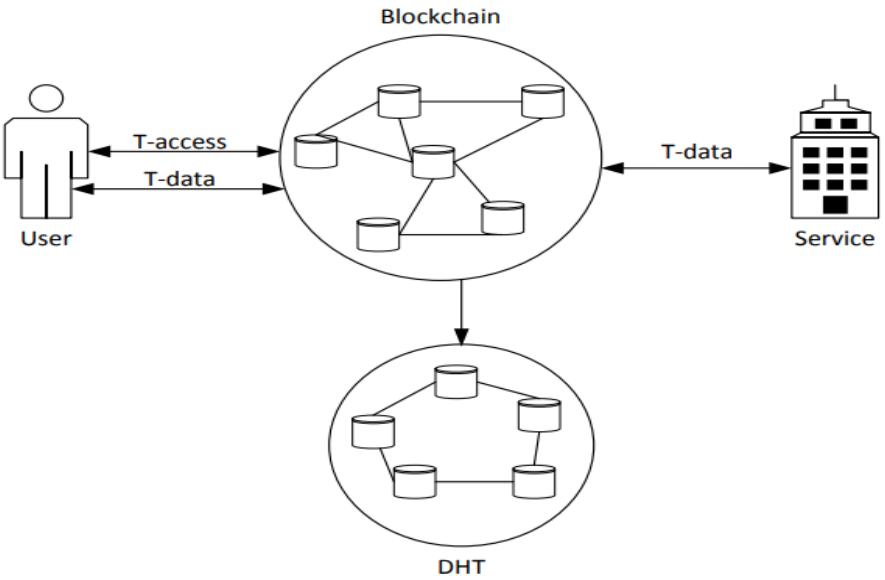

Fig. 2: Overview of Decentralized Permissions System(18)

The user, the business that offers the service, and the Blockchain are the three components of the solution. When a user wishes to provide or take away access to her personal data, Blockchain

acts as a middleman. In this case, Blockchain allows for two kinds of transactions: access transactions and data transactions. Access control management, data storage, and data retrieval are all possible with these transaction types. When a user downloads a new app, a shared identity is generated and transmitted to the Blockchain, together with the rights specified by the user. The so-called Policy contains a list of all the permissions that have been given. An access transaction in the Blockchain sends the shared keys (the user's public key and the service's public key) and the policy.

3.2. Digital Property:

The intellectual property of digital art is linked to a particularly specific application of Blockchain in the field of Big Data. Artists, designers, and creative professionals may readily share their work on the Internet, but maintaining the right to do so with appropriate credit and being properly paid has proved challenging in our digital age. There is no visible way to possess something that can be readily duplicated and completely reproduced without leaving any trace of the original. According to the Ascribe project, the Internet was created with a critical defect in terms of ownership(19). The creator loses ownership of his or her work once it is posted online, or even sold online. That is why Ascribe's mission is to create the Internet's ownership layer for digital material. They're working on a tool for writers that will provide them visibility into how their work circulates throughout the arts(20).

On the Internet, the writers, channels, and customers are all in a tangle. Consumers confront material that isn't accessible for purchase, and creators don't have a consistent method of being properly compensated. Even for distribution networks, the process of licensing and lawfully selling material is arduous. There is still no common method for sharing films, movies, music, pictures and photographs, as well as 2D and 3D digital graphics.

So, what's going on here? The World Wide Web began with basic hyperlinks, laying the groundwork for no discernible difference between what is original and what is copied. People then came up with a method to acknowledge the creator by noting it in the references and attributing the images they copied and utilized. However, this method is far from perfect. People can always find a method to duplicate anything without giving credit, and the creator will never know or be informed. Alternatively, individuals may credit the author, but it will only be a one-way link, thus the author will be unaware that her work has been cited. Worse, individuals may credit someone else's work to someone who isn't the actual creator. As a result, it seems that the primary instrument for creating and distributing digital information (the internet) neglected the requirement for digital property. However, history contradicts this. Ted Nelson created Project Xanadu, the first hypertext project, in 1960(21). The solution to this issue was to include a royalty-based publishing scheme into a system that would offer storage and publication services. This system includes author attribution. When someone utilized another user's data, bi-directional connections were supposed to be created automatically. The project was shut down when it was discovered that this was a complex, non-feasible technology.

Ascribe is now using Blockchain technology to attempt to accomplish the Xanadu objectives by developing a solution for the digital property registration and copy visibility. In terms of visibility, they are attempting to locate all copies of the protected material that are available on the Internet. This may be accomplished by crawling the whole internet and comparing it to the material of the author. This is a similarity search issue for machine learning. When the copies are

discovered, the system creates bi-directional connections automatically. The author must next determine whether she will seek license payments or a takedown request.

When it comes to selling digital art intellectual property, it's not only about selling a copy; it's about selling ownership as well as the right to use, alter, and resell the material. This kind of ownership sale (as opposed to a license sale) requires the execution of a formal contract, as well as the engagement of a lawyer. The concept of utilizing Blockchain to store and sell digital data ownership will be as easy as sending an e-mail with a signature stating that the user has transferred ownership of her material. Ascribe's terms of service are developed in collaboration with experienced attorneys. Accepting the terms of service takes care of the intricacy of the legal licensing and ownership procedures. Blockchain is a public, trustworthy ledger that will protect all users' copyrights. In the event of a disagreement over ownership, the time stamping of the transactions may be used as evidence in court.

4. CONCLUSION

Blockchain has a lot of potential for Big Data's future. The first is that consumers may be able to manage all of their data and transactions in various areas. They may be certain that transactions will be carried out precisely as the protocol directs, obviating the requirement for a trusted third party. This idea may inspire Big Data to develop a solution for storing and managing data on a P2P network in a dispersed way. Blockchain technology has the potential to become a new component of the Big Data ecosystem of tools. In fact, it may play a critical role in data security by allowing users to authenticate themselves, limiting access depending on their needs, documenting data access histories, and properly encrypting data.

Consensus models, the computational expenses of mining blocks, and verifying transactions are all problems that persist. Furthermore, Blockchain applications provide solutions that do not need substantial modifications to current systems or their full replacement. As a result, the transfer will not be simple or quick. However, we are still in the early phases of Blockchain development, and these roadblocks will be removed soon, paving the way for a plethora of fascinating possibilities.

REFERENCES

1. Jain N, Awasthi Y. WSN-AI based Cloud computing architectures for energy efficient climate smart agriculture with big data analysis. Int J Adv Trends Comput Sci Eng. 2019;

2. Mathur G, Ghai W, Singh RK. A totalitarian technique for wormhole detection using big data analytics in iot network. Int J Sci Technol Res. 2020;

3. Gupta D, Rana A, Tyagi S. A novel representative dataset generation approach for big data using hybrid Cuckoo search. Int J Adv Soft Comput its Appl. 2018;

4. Agarwal N, Rana A, Pandey JP. Proxy signatures for secured data sharing. In: Proceedings of the 2016 6th International Conference - Cloud System and Big Data Engineering, Confluence 2016. 2016.

5. Al-Bahri B, Noronha H, Pandey J, Singh AV, Rana A. Evaluate the Role of Big Data in Enhancing Strategic Decision Making for E-governance in E-Oman Portal. In: ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions). 2020.

6. Gupta P, Tyagi N. An approach towards big data - A review. In: International Conference on Computing, Communication and Automation, ICCCA 2015. 2015.

7. Srivastava R, Sharma PK, Das KJM, Manjhi J. A hybrid approach for head and neck cancer using online image guidance and offline adaptive radiotherapy planning. J Radiother Pract. 2019;

8. Hammer S. The Blockchain Ecosystem. SSRN Electron J. 2018;

9. Goyal AK, Singh R, Chauhan G, Rath G. Non-invasive systemic drug delivery through mucosal routes. Artificial Cells, Nanomedicine and Biotechnology. 2018.

10. Niladry G, Ranjit S. Biogenic synthesis of bimetallic nanoparticles using cassia tora leaf extract. Res J Biotechnol. 2020;

11. Goswami L, Kaushik MK, Sikka R, Anand V, Prasad Sharma K, Singh Solanki M. IOT Based Fault Detection of Underground Cables through Node MCU Module. In: 2020 International Conference on Computer Science, Engineering and Applications, ICCSEA 2020. 2020.

12. Brody P, Pureswaran V. Device democracy: Saving the future of the Internet of Things IBM. IBM Glob Bus Serv Exec Rep. 2015;

13. Rabah K, Research M, Nairobi K. Convergence of AI, IoT, Big Data and Blockchain: A Review. Lake Inst J. 2018;

14. Yue L, Junqin H, Shengzhi Q, Ruijin W. Big Data Model of Security Sharing Based on Blockchain. In: Proceedings - 2017 3rd International Conference on Big Data Computing and Communications, BigCom 2017. 2017.

15. Sun H, Hua S, Zhou E, Pi B, Sun J, Yamashita K. Using ethereum blockchain in Internet of Things: A solution for electric vehicle battery refueling. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2018.

16. Rainie L, Duggin M. Privacy and Information Sharing. Pew Res Cent Internet Proj. 2016;

17. Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. In: Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015. 2015.

18. Fernandes E, Rahmati A, Jung J, Prakash A. Decentralized Action Integrity for Trigger-Action IoT Platforms. In 2018.

19. McConaghy T, Holtzman D. Towards An Ownership Layer for the Internet. Ascribe. 2015.

20. Goswami G, Goswami PK. Artificial Intelligence based PV-Fed Shunt Active Power Filter for IOT Applications. In: Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020. 2020.

21. Rosenzweig R. The Road to Xanadu: Public and Private Pathways on the History Web. J Am Hist. 2001;