RESEARCHERID
THOMSON REUTERS

[Kayasth *et al.*, 7(9): September, 2018]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A STUDY OF ISSUES AND CHALLENGES FACE BY BLOCKCHAIN TECHNOLOGY

Dr. Manish M. Kayasth[1], Jagin M. Patel[2]

[1]Assistant Professor and HOD, Udhna Citizen Commerce College & SPB College of Business Administration & SDHG College of BCA & IT, Surat, Gujarat, India

[2]Assistant Professor, M. K. Institute of Computer Studies, Bharuch, Gujarat, India

ABSTRACT

Blockchain is an emerging technology that is secure, safe, and bug-free. This cutting-edge technology operates in both distributed and decentralised modes. Blockchain is a distributed database whose records are highly secure, immutable, and transparent to all stakeholders. We may utilise the features and benefits of this technology in hybrid mode, which combines it with other existing technologies. The merging of such multi-technologies will result in smart systems that provide additional automation features to industry and society. In this paper, we will explore blockchain technology, its features, security aspects, numerous concerns and obstacles, as well as its applications. Blockchain is a decentralised technology. It has a significant ability to solve business difficulties.

Cryptography protects the records in a blockchain transaction, and each transaction is linked to previous transactions or records. Node-based algorithms validate blockchain transactions. A single entity cannot initiate a transaction. Blockchain offer transparency, allowing each participant to observe transactions at any moment. Smart contracts provide safe transactions, which helps to avoid third-party disturbance. The key features of blockchain are decentralisation and immutability. Faster transactions, validation in seconds, and so on.

A blockchain is simply a distributed database of records or a public ledger, that contains all transactions or digital events that have been conducted and shared by participating parties. Each transaction in the public ledger is validated by a majority of the system's participants. Once entered, information cannot be deleted. The blockchain includes a precise and verifiable record of every transaction ever made. The most popular example of blockchain technology is Bitcoin, a decentralised peer-to-peer digital currency. The digital currency Bitcoin is very controversial, but the underlying blockchain technology has worked brilliantly and has a wide range of uses in both the financial and non-financial worlds.

This paper describes blockchain technology and some compelling specific applications in both the financial and non-financial sectors. We then look at the challenges ahead and business opportunities in this fundamental technology that is all set to revolutionize our digital world.

Keywords: Blockchain, Characteristics, Challenges, Security, Advantages.

1. INTRODUCTION

The concept of Blockchain technology was first introduced in 2008 by Satoshi Nakamoto[1], which outlined the key principles and mechanics of blockchain technology and served as the foundation for the development of cryptocurrencies like Bitcoin. Bitcoin is as much about "online" as it is about currency, with numerous applications in and developing mobile commerce [2]. Bitcoin focuses on online transactions [3]. It can function as a platform for financial information [4].

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Blockchain technology is a way to structure data without the need for a central authority. It is a distributed database that hosts a continuously growing number of records. The database stores records in blocks rather than collating them in a single file. Each block is chained to the next block, in linear, chronological order, using a cryptographic technique. The records in this technology cannot be revised. Any attempt to change those records is visible to all involved participants. This mechanism enables blockchains to function as ledgers that can be shared and confirmed by anybody with the necessary permissions [5]. These distributed ledgers can be spread across multiple places.

Blockchain architecture is the foundational structure that enables the decentralized and secure operation of blockchain networks. It comprises a set of rules, protocols, and components that work in tandem to maintain the integrity of the distributed ledger. The architecture ensures transparency, immutability, and consensus in recording and validating transactions across a network of nodes.

Blockchain is a technology that redefines trust in next-generation systems. It promotes the idea of conducting any form of transaction without the use of a mediator. Mediators, such as corporations and governments, nearly invariably operate as central entities, receiving, processing, and storing transactions. All of the trust we place in any system is in the mediators, who are required to handle transactions in accordance with proper business logic. Mediators have full control over data security and privacy. Technically, Blockchain is a distributed database that resides on a peer-to-peer network (Fig. 1). This peer-to-peer network serves as the system's backbone because each node in the network is on the same level as the others. Although nodes can take many different forms, there is no single core node that serves as an authority. Every node keeps a local copy of the blockchain. If a majority of nodes agree on the transaction's legitimacy, the transaction is considered valid. [6].

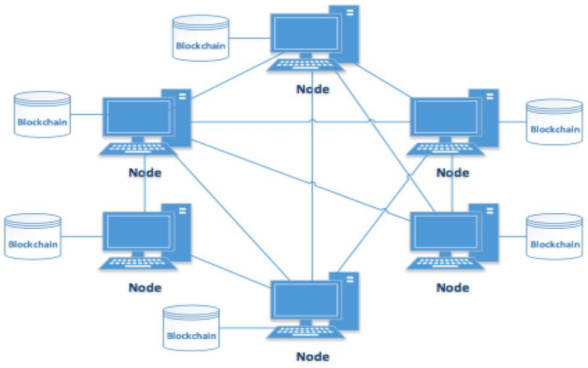

Fig. 1. Blockchain P2P Network [6]

Richard and Owen [7] addresses the limitations and vulnerabilities of current reputation systems, both in centralized and peer-to-peer (P2P) networks. The authors propose a new reputation system based on blockchain technology, which aims to solve existing issues and prevent attacks that can occur in traditional reputation systems. The proposed system is applicable to both P2P and centralized networks and provides a method for accurate and trustworthy calculation of reputation scores, without the need for a central authority. The use of blockchain technology ensures the immutability of transactional records and prevents the creation of multiple identities and fraudulent ratings. The paper discusses various attacks on decentralized reputation systems and outlines measures that prevent such attacks from depriving the reputation system of its usefulness. The proposed system shows promise in resolving many of the unanswered questions of current reputation systems, and the authors provide valuable insights and suggestions for future research that can further optimize the system.

Yong and Wang [8] discusses the potential of blockchain technology in revolutionizing intelligent transportation systems (ITS). The authors propose a blockchain-based ITS (B2ITS) framework that can establish a secured, trusted, and decentralized ITS ecosystem. They outline a seven-layer conceptual model for blockchain in an ITS context and address key research issues in B2ITS. They also discuss the relationship between B2ITS and parallel transportation management systems (PtMS). The authors present a case study of a blockchain-based real-time ride-sharing service as an example of B2ITS application. They emphasize the importance of security, trust, and decentralization in maintaining the overall stability, profitability, and effectiveness of the ITS ecosystem.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Michael et. al. [9] cover blockchain technology and its applications beyond Bitcoin. It explained that a blockchain is a distributed database of records or a public ledger of transactions that is verified by consensus among participants in the system. The main hypothesis presented is that blockchain technology establishes a system of creating a distributed consensus in the digital world, allowing for the creation of a democratic and scalable digital economy. It also document describes the history and workings of Bitcoin and how it uses blockchain technology. It also discusses the advantages of blockchain technology, such as its ability to revolutionize the digital world by enabling a distributed consensus and preserving the privacy of digital assets and parties involved.

Blockchain literature is abundant and comes from a variety of sources, including blogs, wikis, forum postings, codes, conference proceedings, and journal publications. Tschorsch et al. [10] conducted a technical survey on decentralised digital currencies, including Bitcoin.

2. CORE ASPECT OF BLOCKCHAIN

Blockchain contains the following core aspects.
Decentralization**:** In traditional centralised transaction systems, each transaction must be certified by a central trusted agency, leading to cost and performance constraints on central servers. In contrast to centralised modes, blockchain eliminates the requirement for third parties. Blockchain's consensus algorithms provide data consistency across diverse networks.

Persistency: Transactions can be validated fast, and invalid transactions will not be accepted. Once a transaction is on the blockchain, it is nearly hard to erase or rollback. Blocks containing invalid transactions might be identified instantly.

Anonymity: Every user may communicate with the blockchain using a created address that does not reveal the user's real identity. Blockchain cannot offer full anonymity owing to inherent constraints. Many methods have been suggested to improve the anonymity of blockchain.

Miners[11] used zero-knowledge proof. Here researcher uses a list of valid coins to validate transactions, rather than requiring a digital signature. Sasson et. al. [12] used zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs). They create decentralised anonymous payment schemes (DAPS). A DAP scheme allows users to pay one other anonymously by hiding the payment's origin, destination and transferred amount. Tim et. al. [13] employs decryption mixnets to shuffle addresses.

3. WHERE BLOCKCHAIN CAN BE APPLIED?

Blockchain technology may provide new opportunities to reduce transaction costs dramatically and decrease transaction settlement time. It has the potential to transform and disrupt a multitude of industries, from financial services to the public sector to healthcare. As a result, a number of venture capital firms and large enterprises are investing in blockchain technology research and trials to re-imagine traditional practices and business models.

A major advantage of blockchain technology is its distributed nature. A blockchain allows parties to transact directly with each other through a single distributed ledger, thus eliminating one of the needs for centralized transaction processors. In addition to being efficient, the blockchain has other unique characteristics that make it a breakthrough innovation.

Currently, most blockchains are used in the financial domain, and more and more applications for different fields are appearing. Traditional industries could take blockchain into consideration and apply blockchain into their fields to enhance their systems. At the same time, the upcoming industry could make use of blockchain to improve their performance [14].

Michael et. al. [9] highlights the potential applications of blockchain technology in both financial and non-financial sectors, including smart contracts, smart property, and various other non-financial applications.
Blockchain can be utilized for a variety of financial services, including digital assets, remittances, and online payments [15]. It has applications in smart contracts [16], IoT [17], reputation systems [18], and security services [19].
Businesses that require high levels of reliability, as well as honesty, can use blockchain to attract clients. Blockchain technology eliminates the possibility of a single point of failure due to its distributed nature.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Financial services**:** Several stock exchanges across the world are piloting a blockchain platform that allows for private securities. Furthermore, a number of institutions are considering use cases for trade financing, cross-border payments, and other financial activities. BlockChain's distributed ledger feature, combined with its security, makes it a particularly attractive solution for solving existing financial and non-financial business concerns [20].

Consumer and industrial products**:** Companies are investigating the use of blockchain to digitise, trace the origins, and history of transactions in different commodities.
Life sciences and healthcare**:** Healthcare organisations are researching the use of blockchain to ensure the integrity of electronic medical records, medical bills, claims, and other documents.

According to a World Economic Forum survey[21], blockchain technology will alter financial services, with at least 10% of global GDP expected to be housed on platforms by 2025. A blockchain can replace any intermediary that maintains a register or facilitates transactions between parties. Using this method, fund promoters might distribute fund shares directly, with no intermediaries. Blockchain technology would increase the efficiency of trade and post-trading operations, improve regulatory control, and eliminate the need for several middlemen. The technology makes transactions more transparent, practically instantaneous, and eliminates the need to trust a single entity. Blockchain technology is a trending technology that would disrupt most company structures, prompting businesses to reassess their long-term strategic plans.

Blockchain technology continues to be used for a variety of purposes, including intellectual property protection, traceability in the supply chain, identity validation, insurance, international payments, IOT, patient privacy in medical care, and prediction markets [22].

Blockchain is a type of Distributed Ledger Technology (DLT) that consists of a chain of blocks that hold an ever-growing digital list of data records without the need for a central server and are configured in such a way that they cannot be edited or updated. Blockchain technology enables safe tracking of transactions, including money, property, information, and authorization rights, without the need for a third-party middleman like a bank [1, 23, 24, 25]

4. SECURITY FEATURES

Blockchain technology, developed to safeguard and decentralise information and transactions, is primarily used to produce cryptocurrencies like Bitcoin [1]

Blockchain technology will provide full transaction security. A block should record each transaction; it will function as a record book. Once a transaction is completed, a block is added to the blockchain as a permanent database. If a block is completed, a new block is either added to it or generated.

The use of cryptographic techniques, such as hashing for data integrity and digital signatures for authentication, played a crucial role in securing the information stored on the blockchain. Each transaction in a blockchain should be recorded in a ledger, and users should only be able to read the information from it.

Another form of security feature is the chain of blocks. In blockchain, each block should have a hash value. These blocks are linked together by their previous hash. If an attacker comes to fix the data, the hash will change, affecting the entire chain. As a result, sensitive data will be better protected.

5. CHALLENGES

Though the blockchain system offers enormous potential for the development of future Internet networks, it faces numerous technological obstacles. Blockchain technology is still in the testing phase, and there are various implementation concerns that must be addressed before establishing a Blockchain-free cryptographically safe system. Swan [23] lists various technical hurdles and constraints for adapting Blockchain technology in the future. Koteska et. al. [6] reviewed many Blockchain implementation quality challenges.
This section summarises the most frequent Blockchain quality concerns discovered in this investigation.

1. Scalability:

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Scalability is a major concern. The amounts of transactions are increasing day by day. Most of the companies were suggesting blockchain for their transaction process.

Scalability is one of the most hard aspects of Blockchain deployments. To achieve theoretically proven security, Blockchain implementations must have a high number of complete nodes. Otherwise, the implementation may result in a less decentralised system, as with Bitcoin. The scalability restrictions of the Blockchain are related to the size of the data on the blockchain, the transaction processing rate, and the latency of data transfer. However, the consensus mechanism has an effect on the latency between transaction submission and confirmation. For example, the duration between the transaction submission and confirmation on Bitcoin is approximately 1 hour (10-minute block interval per block and 6-block confirmations), and around 3 minutes on Ethereum (14-second block interval per block and 12-block confirmation) [6].

2. Privacy Leakage:
One issue related to Blockchain privacy is the problem of multiple addresses, such as Researchers' cluster addresses belonging to the same user in the Bitcoin system [26]. Address clustering is used to track the economic activity of the same users. The purpose is to locate all addresses involved in the transaction that belong to the same user [27, 28]. The authors in [29] discovered that some Bitcoin addresses can be mapped to IP addresses by analysing the transaction activity.

Blockchain provides anonymity through public and private keys. Users use their private and public keys without revealing their real identities. Blockchain cannot ensure transactional privacy as the values of all the transactions and balances for each public key are publicly visible [16, 30].

3. DDoS (Distributed Denial of Service) Attack:
A DDoS attack is an attack that is designed to target a specific system, such as a computer, website, server, or other network resources. As a result, inbound messages and connections to the target system may slow down, fail, or shut down. DDoS attacks pose a serious threat to business in Blockchain. However, preventing such an attack is almost difficult. A flow analytic device is a frequent solution for DDoS attacks. This device will monitor and react to the attackers. This will tell you what step to take next. This device will additionally assist in clearing the traffic [6].

4. Integrated Cost Problem**.** It will incur significant costs, including time and money, to update an old system, particularly if it is an infrastructure. One must be sure that this creative technology not only creates economic benefits and meets oversight criteria, but also bridges with traditional organisations, and it always encounters problems from internal organisations that are now in place [22].

Other issues are Throughput issues, Latency issues, Size and bandwidth issues, Data malleability issues, and Authentication issues.

6. CONCLUSION

A blockchain builds on existing networks, cryptographic principles, and recordkeeping technology, but employs them in a novel way. Once a blockchain is built and widely used, it may be difficult to update it. Once data is recorded on a blockchain, it is usually retained indefinitely, even if there is an error. Applications that use the blockchain ensure that the actual blockchain data cannot be changed by treating subsequent blocks and transactions as updates or modifications to previous blocks and transactions. Blockchain technology is still in its early stages, and organisations should regard it as any other technological solution, employing it only when necessary.

Blockchain technology has the potential to solve practical business challenges in a variety of industries. It ensures trust, immutability and transparency, and provides additional security for Internet transactions. It is a distributed database technology that enables decentralised transaction and data management. Modern Blockchain systems must prioritise security, privacy, throughput, size and bandwidth, performance, usability, data integrity, and scalability. However, these quality traits present a number of issues that must be handled.

To better understand the current research on the subject of Blockchain implementation quality, we examined current quality challenges in Blockchain implementations and established Blockchain quality attributes.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

According to the research, this topic is yet immature. The results show that the Blockchain implementations should be enhanced.

7. FUTURE WORK

The future of blockchain will be to combine it with AI to provide cyber security, by training ML (Machine Learning) algorithms to carry out real-time threat identification as well as continually learn about attacker behaviour. The decentralised nature of blockchains can reduce the inherent risk of centralised databases. AI can improve the efficiency of blockchain significantly more than humans or traditional computing.

Recent advancements in blockchain technology are opening up new possibilities for artificial intelligence applications. AI technology has the potential to help tackle a variety of blockchain difficulties.

REFERENCES

1. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008).
2. Hurlburt, G.F., Bojanova, I.: Bitcoin: benefit or curse? IT Prof. 16, 10–15 (2014)
3. Turpin, Jonathan B. "Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework." Ind. J. Global Legal Stud. 21 (2014): 335.
4. Cusumano, M.A.: The bitcoin ecosystem. Commun. ACM 57, 22–24 (2014)
5. Arsov, Doc. "Periodic Table of Cryptocurrencies: Blockchain Categorization." Available at SSRN 3095169 (2017).
6. Koteska, Bojana, Elena Karafiloski, and Anastas Mishev. "Blockchain implementation quality challenges: a literature." In SQAMIA 2017: 6th workshop of software quality, analysis, monitoring, improvement, and applications, vol. 1938, pp. 8-8. 2017.
7. Dennis, Richard, and Gareth Owen. "Rep on the block: A next generation reputation system based on the blockchain." In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 131-138. IEEE, 2015
8. Yuan, Yong, and Fei-Yue Wang. "Towards blockchain-based intelligent transportation systems." In 2016 IEEE 19th international conference on intelligent transportation systems (ITSC), pp. 2663-2668. IEEE, 2016.
9. Crosby, Michael, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. "Blockchain technology: Beyond bitcoin." Applied Innovation 2, no. 6-10 (2016): 71.
10. Tschorsch, Florian, and Björn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." IEEE Communications Surveys & Tutorials 18, no. 3 (2016): 2084-2123.
11. Miers, Ian, Christina Garman, Matthew Green, and Aviel D. Rubin. "Zerocoin: Anonymous distributed e-cash from bitcoin." In 2013 IEEE Symposium on Security and Privacy, pp. 397-411. IEEE, 2013.
12. Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. "Zerocash: Decentralized anonymous payments from bitcoin." In 2014 IEEE symposium on security and privacy, pp. 459-474. IEEE, 2014.
13. Ruffing, Tim, Pedro Moreno-Sanchez, and Aniket Kate. "Coinshuffle: Practical decentralized coin mixing for bitcoin." In Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19, pp. 345-364. Springer International Publishing, 2014.
14. Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. "An overview of blockchain technology: Architecture, consensus, and future trends." In 2017 IEEE international congress on big data (BigData congress), pp. 557-564. Ieee, 2017.
15. Foroglou, George, and Anna-Lali Tsilidou. "Further applications of the blockchain." In 12th student conference on managerial science and technology, vol. 9. 2015.
16. Kosba, Ahmed, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." In 2016 IEEE symposium on security and privacy (SP), pp. 839-858. IEEE, 2016.
17. Zhang, Yu, and Jiangtao Wen. "An IoT electric business model based on the protocol of bitcoin." In 2015 18th international conference on intelligence in next generation networks, pp. 184-191. IEEE, 2015.
18. Sharples, Mike, and John Domingue. "The blockchain and kudos: A distributed system for educational record, reputation and reward." In Adaptive and Adaptable Learning: 11th European Conference on

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Technology Enhanced Learning, EC-TEL 2016, Lyon, France, September 13-16, 2016, Proceedings 11, pp. 490-496. Springer International Publishing, 2016.
19. Noyes, Charles. "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning." arXiv preprint arXiv:1601.01405 (2016).
20. Crosby, Michael, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. "Blockchain technology: Beyond bitcoin." Applied Innovation 2, no. 6-10 (2016): 71.
21. Benjamin Collette, Simon Ramos et al., "Impacts of the Blockchain on fund distribution", World Economic Forum, September 2015.
22. Lin, Iuon-Chang, and Tzu-Chun Liao. "A survey of blockchain security issues and challenges." Int. J. Netw. Secur. 19, no. 5 (2017): 653-659.
23. Swan M. Blockchain: Blueprint for a New Economy. " O'Reilly Media, Inc."; 2015
24. Yli-Huumo, Jesse, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. "Where is current research on blockchain technology?—a systematic review." PloS one 11, no. 10 (2016): e0163477.
25. Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services 14, no. 4 (2017).
26. Herrera-Joancomartí, Jordi, and Cristina Pérez-Solà. "Privacy in bitcoin transactions: new challenges from blockchain scalability solutions." In Modeling Decisions for Artificial Intelligence: 13th International Conference, MDAI 2016, Sant Julià de Lòria, Andorra, September 19-21, 2016. Proceedings 13, pp. 26-44. Springer International Publishing, 2016.
27. Reid, Fergal, and Martin Harrigan. An analysis of anonymity in the bitcoin system. Springer New York, 2013.
28. Androulaki, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. "Evaluating user privacy in bitcoin." In Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17, pp. 34-51. Springer Berlin Heidelberg, 2013.
29. Koshy, Philip, Diana Koshy, and Patrick McDaniel. "An analysis of anonymity in bitcoin using p2p network traffic." In Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18, pp. 469-485. Springer Berlin Heidelberg, 2014.
30. Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. "A fistful of bitcoins: characterizing payments among men with no names." In Proceedings of the 2013 conference on Internet measurement conference, pp. 127-140. 2013.