"Unravelling the Challenges: A Deep Dive into the Problems of Blockchain Technology"

Dr. Gopal Pardesi[1], Diksha Pardeshi[2]

Associate Professor, Dept. of Information Technology, Thadomal Sahani College of Engineering, Maharashtra, India
Final-year B.E.-IT, Shree L.R. Tiwari College of Engineering, Maharashtra, India

---***---

Abstract - *Blockchain technology has grown in popularity in recent years as a viable solution to a variety of challenges in numerous sectors. It has improved transparency, security, and efficiency in a variety of applications, including banking, healthcare, supply chain management, and voting systems. However, the adoption of blockchain technology is fraught with difficulties and constraints. This research paper provides an in-depth examination of the issues surrounding blockchain technology, including scalability, security, interoperability, legislation, governance, and environmental effect. We investigate the underlying causes of these challenges, as well as the current status of research and potential remedies.*

Key words: Blockchain scalability, Transaction throughput, Confirmation time, Network congestion, Interoperability, Network latency, Consensus algorithms, Smart contract vulnerabilities.

I INTRODUCTION

Blockchain technology is a distributed ledger system that enables safe and transparent transactions without the use of middlemen. It is frequently connected with cryptocurrencies like Bitcoin and Ethereum, although its uses extend well beyond digital currency. By boosting trust, efficiency, and transparency, blockchain technology has the potential to revolutionise many sectors. However, the adoption of blockchain technology is fraught with difficulties and constraints. We intend to present a complete assessment of the challenges connected with blockchain technology, their basic causes, and potential solutions to these concerns in this research study.

II LITERATURE SURVEY

Blockchain comes with the promise of being a disruptive technology with the potential for novel ways of interaction in a wide range of applications. Following broader application, scholarly interest in the technology is growing, though an extensive analysis of blockchain applications from a governance perspective is lacking to date. This research pays special attention to the governance of blockchain systems and illustrates decision problems in 14 blockchain systems from four application domains. Based on academic literature, semi-structured interviews with representatives from those organizations, and content analysis of grey literature, common problems in blockchain governance have been singled out and contextualized.[1]

Recorded healthcare data by using electronic health record (EHR) can be shared with numerous medical management units, hospitals, health centres, laboratory for identification of disease. Regardless of sharing data, it is vulnerable because it could be tempered or harmed as security and privacy have not been promised. In current time, it is shown that medical data is using cloud for storage, but there is also security, privacy and trust which has not been guaranteed. Therefore, researchers have come up with the solution known as blockchain technology to preserve data. By integrating cloud with this technology, data becomes invulnerable. As matter of fact, blockchain-based cloud technology can resolve lot of issues concerning healthcare industry.[3]

In the past few years block chain has gained lot of popularity because blockchain is the core technology of bitcoin. Its utilization cases are growing in number of fields such as security of Internet of Things (IoT), banking sector, industries and medical centres. Moreover, IoT has expanded its acceptance because of its deployment in smart homes and city developments round the world. Unfortunately, IoT network devices operate on limited computing power with low storage capacity and network bandwidth. Thus, they are extra close to attacks than other end-point devices such as cell phones, tablets, or PCs. This paper focus on addressing significant security issues of IoT and maps IoT security issues in contradiction of existing solutions found in the literature. Moreover, issues that are not solved after implementation of blockchain are highlighted.[4]

III Problems with Blockchain Technology

Although blockchain technology has several potential benefits such as decentralization, security, transparency, and immutability, it also faces some significant challenges. Some of the major problems with blockchain technology include:

Problem 1: Scalability

One of the most serious issues with blockchain technology is scalability. The existing blockchain infrastructure can only handle a limited number of transactions per second (TPS), which is significantly less than the capacity of traditional payment systems like Visa and Mastercard. This restriction is mostly due to the blockchain technology's consensus process, which needs every node in the network to validate every transaction. The network gets slower and less efficient as the number of nodes and transactions grows.

Sharding allows blockchain networks to handle a greater number of transactions in parallel, increasing network throughput and decreasing transaction confirmation times. Furthermore, sharding can lower the computational and storage needs of running a network node.

Layer 2 solutions decrease the load on the underlying blockchain network by processing transactions off-chain while maintaining the system's security and integrity. Payment channels, state channels, sidechains, plasma, and rollups are all part of it. Layer 2 solutions are viewed as a viable option to increase blockchain network scalability while retaining security and decentralisation.

Changing a blockchain network's consensus algorithm can have serious consequences for its performance, security, and decentralisation.

Problem 2: Security

Another significant issue with blockchain technology is security. While blockchain is often regarded as a safe and impenetrable system, it is nevertheless subject to a variety of assaults, including 51% attacks, double-spending attacks, and Sybil attacks. Furthermore, smart contract flaws have been exploited in a number of high-profile attacks, including the DAO assault and the Parity wallet compromise.

The development of safe and trustworthy smart contracts is critical to the success and acceptance of blockchain technology. Better smart contract development practises increase smart contract quality and security. Upgraded blockchain consensus processes are critical for increasing the scalability, security, and decentralisation of blockchain networks. These updates frequently need considerable modifications to the network's underlying architecture and must be carefully planned and tested to ensure that they do not create new vulnerabilities or decrease overall system security.

Improved cryptography also contributes to the security, privacy, and integrity of blockchain data. These improved cryptographic approaches are continually changing, and developers must keep up with the newest advances to maintain the security and resilience of their blockchain systems.

Problem 3: Interoperability

Interoperability refers to the capacity of multiple blockchain networks to smoothly interact and transact with one another. The existing blockchain ecosystem, on the other hand, is highly fragmented, with several blockchain networks employing disparate protocols and standards. This fragmentation makes it difficult to transmit value and data between blockchains. Interoperability is critical for broad adoption of blockchain technology and the development of a more integrated and efficient global economy.

Standardisation can assist to guarantee that diverse blockchain networks can connect and interact with one another in a smooth manner, increasing the efficiency and value of blockchain technology. Interoperability protocols are a critical component in enhancing blockchain technology compatibility. compatibility standards promote blockchain technology compatibility. Interoperability protocols allow various blockchain networks to effortlessly communicate and interact with one another, which can contribute to a more linked and efficient global economy.

Bridging mechanisms can assist in the development of a more integrated and efficient global economy. To guarantee that their blockchain applications are interoperable and durable, developers must remain up to speed on the newest bridge methods.

Problem 4: Regulation and Governance

In the blockchain sector, regulation and governance are major concerns. Because blockchain technology is still in its early stages, governments all over the world are attempting to find out how to control and oversee it. Lack of standardisation, ambiguous legal status, lack of consumer protection, governance concerns, and interoperability hurdles are the key regulatory and governance issues in the blockchain business.

The aforementioned issues can be addressed by implementing self-governance, which means that the blockchain network should regulate itself without the need for a central authority or middleman. Smart contracts may also be used to automate and transparently enforce compliance procedures. Blockchain firms may create confidence with consumers and regulators by adhering to regulatory regulations, allowing them to operate legally and effectively in the burgeoning blockchain market.

Regulatory sandboxes may be especially effective for encouraging innovation, reducing regulatory ambiguity, and providing regulatory direction. It increases collaboration and consumer protection. The use of blockchain-based registries improves security, transparency, efficiency, and interoperability. They can be constructed to be decentralised, with no single point of failure or control, resulting in a more robust and democratic system.

Smart contracts may be used to automate regulatory compliance operations such as tax information reporting and compliance certificate checking. This may decrease the burden on businesses while also ensuring compliance is enforced in a transparent and effective manner.

5. Trust among users

Because blockchain technology is a decentralised and trust less system that depends on encryption and consensus procedures to confirm transactions, user trust is a crucial issue for it. However, a lack of trust among users can rise to problems such as fraudulent transactions, harmful attacks, and arguments about transaction legality.

Reputation systems can help consumers build trust by awarding ratings or scores based on previous transactions or behaviour. This can aid in the identification of trustworthy users and the prevention of fraudulent activities. It has the potential to promote good behaviour in blockchain networks.

Decentralised reputation systems may be designed to prevent a single entity from manipulating the score system for their own gain, resulting in a more democratic and transparent system. Decentralised identity management (DID) is a new blockchain application that seeks to offer users more control over their personal information and online identities. Decentralised identity management solutions leverage blockchain technology to generate a self-sovereign identity (SSI) that the user owns and controls. DID has the potential to enhance privacy, security, and access to services and opportunities.

Smart contract escrow services can be used to hold payments or assets until specific criteria, such as the delivery of products or the fulfilment of a service, are satisfied. This can aid in the prevention of fraudulent transactions and the establishment of confidence between buyers and sellers. Intermediary services, or third-party entities, can be used to build trust among users. These services can serve to prevent fraudulent conduct and build trust between users by providing dispute resolution, verification, or insurance.

Blockchain technology can assist to establish a more secure, transparent, and trustworthy system for all users by utilising reputation systems, decentralised identity management, smart contract escrow services, transparency and auditability, and intermediary services.

6. Financial resources

Blockchain technology has the potential to solve the problem of financial resources by facilitating access to money, financial inclusion, and financial transaction transparency.

Blockchain technology can help solve the problem of financial resources by expanding financial inclusion, enhancing transparency and efficiency in financial transactions, and increasing access to finance. Blockchain technology can assist to establish a more egalitarian and accessible financial system for all by utilising DeFi, tokenization, smart contracts, transparent financial transactions, and crowdfunding.

7. Skills gap

The scarcity of trained people with the essential competence to create, deploy, and maintain blockchain-based solutions is referred to as the blockchain skills gap problem. Education and training, professional certifications, cooperation and collaborations, community support, and automation and tools may all help to close the blockchain skills gap. The blockchain sector can continue to expand and innovate through cultivating a competent workforce, resulting in a more robust and inclusive technological environment.

8. Public perception

Due to its association with cryptocurrencies, which have been connected with fraudulent schemes and criminal activity, the public impression of blockchain technology can be challenging.

To improve public perception of blockchain technology, a mix of education and awareness, transparency and regulation, real-world applications, good media coverage, and user experience improvements is required. By resolving these concerns, blockchain technology may be more broadly used and seen as a valuable instrument for social and economic progress.

9. Energy consumption

The energy consumption issue with blockchain technology stems from the consensus technique employed in many blockchain networks, such as proof of work (PoW), which necessitates a substantial amount of computing power and energy consumption.

The energy consumption issue necessitates a multifaceted response that involves switching to energy-efficient consensus procedures, developing energy-efficient infrastructure, employing off-chain transactions, scaling solutions, and using carbon credits. Blockchain technology may become more sustainable and ecologically friendly by incorporating these solutions, while maintaining providing the benefits of decentralisation, security, and transparency.

10. Privacy problem

Because blockchain technology is designed to be irreversible and transparent, users may have privacy concerns. Blockchain technology's privacy challenge necessitates a mix of technological solutions, such as ZKPs and encrypted transactions, as well as governance solutions, such as private and permissioned blockchains and self-sovereign identities. Blockchain technology may give the benefits of decentralisation and security while also maintaining user privacy by deploying these solutions.

11.Inefficient technology design

Blockchain networks are not intended to be scalable or efficient, which might result in long transaction times and large transaction costs. Blockchain's inefficient technology design necessitates a mix of technical improvements, including layer-2 scaling solutions, sidechains, sharding, optimised blockchain architecture, and hardware optimisation. Blockchain technology may become more efficient, scalable, and cost-effective by incorporating these solutions, while maintaining providing the benefits of decentralisation, security, and transparency.

IV RESEARCH METHODOLOGY

A. THE SURVEY QUESTIONS

This study utilizes a survey (online as well as off-line) that was conducted between 2022 to 2023. The survey explored various aspects of blockchain and covered a large set of questions.

B. DATA CLEANING AND VALIDATION

On the first dataset, we went through a careful information cleaning and clearance procedure to ensure the quality and authenticity of the survey data. The technique was mostly automated using the R programming package. We physically evacuated suspicious information routes. To begin the information cleaning process, we have removed any duplicate entries that may have appeared throughout the information sending out method. We also corrected a number of obvious errors that may be attributed to the overview strategy or information transmission mechanism.

We completed manual information cleansing question by question after this primer advance. Following the first cleaning, we confirmed the authenticity of the information using a large number of approval instances that we discovered based on a local examination of all the survey questions. The approval instances discovered several irrational, inconceivable, and invalid combinations of replies, rendering some data sections invalid and consequently removing them from the dataset.

C. Data Analysis

The data analysis process was conducted using R and SPSS software environment.

D. Hypothesis testing

Hypotheses were tested using Chi square test.

Hypothesis 1: Does Layer 2 solutions enhance the capabilities of blockchain network.

H0 Null Hypothesis: less than 70% blockchain networks use Layer 2 solutions to enhance their capabilities (H0: $p < .70$).

H1 Alternate Hypothesis: 70% or more blockchain networks use Layer 2 solutions to enhance their capabilities (H1: $p \geq .70$).

This hypothesis has been tested by using the acceptance of blockchain project managers, blockchain architects and blockchain consultants. It is seen that 81.90% of them have agreed to use Layer 2 solutions to enhance the capabilities of blockchain networks as shown in Figure 1.

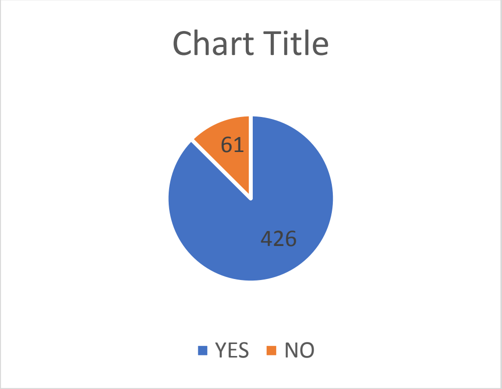

Figure 1:Use of Layer 2 solutions

χ2 value is found out to be 38.18 which is greater than the table value 3.84 at 5% level of significance. Hence, Null hypothesis is rejected and alternate hypothesis is accepted.

Hypothesis 2: Does the overall security of blockchain networks be increased by upgrading the consensus mechanism.

H0 Null Hypothesis: less than 70% blockchain networks upgrade the consensus mechanism to increase the security of transactions. (H0: p < .70).

H1 Alternate Hypothesis:70% or more blockchain networks regularly upgrade the consensus mechanism to increase the security of transactions. (H1: p ≥ .70).

This hypothesis has been tested by using the acceptance of blockchain project managers, blockchain architects and blockchain consultants. It is seen that 77.61% of them have agreed to regularly upgrade the consensus mechanism to enhance the security of blockchain networks as shown in Figure 2.

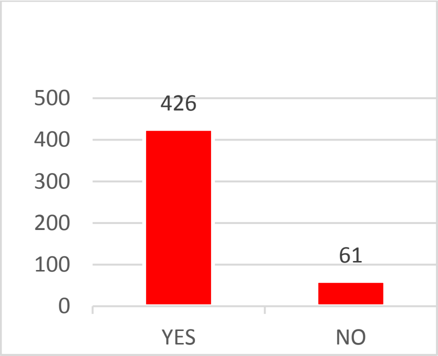

Figure 2: Upgrade of consensus mechanism

χ2 value is found out to be 10.47 which is greater than the table value 3.84 at 5% level of significance. Hence, Null hypothesis is rejected and alternate hypothesis is accepted.

Hypothesis 3: Can use of cross-chain bridges enable interoperability between different blockchain networks.

H0 Null Hypothesis: less than 70% blockchain networks use cross-chain bridges to enable interoperability between different blockchain networks. (H0: p < .70).

H1 Alternate Hypothesis: 70% or more blockchain networks use cross-chain bridges to enable interoperability between different blockchain networks. (H1: p ≥ .70).

This hypothesis has been tested by using the acceptance of blockchain project managers, blockchain architects and blockchain consultants. It is seen that 87.47% of them have agreed to use cross-chain bridges to enable interoperability between different blockchain networks as shown in Figure 3.

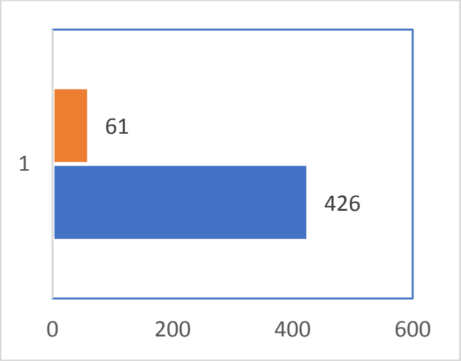

Figure 3: Use of cross-chain bridges

χ2 value is found out to be 67.42 which is greater than the table value 3.84 at 5% level of significance. Hence, Null hypothesis is rejected and alternate hypothesis is accepted.

Hypothesis 4: Does decentralized identity management has the potential to improve trust in blockchain networks

H0 Null Hypothesis: less than 70% blockchain networks use decentralized identity management to improve trust in their networks (H0: p < .70).

H1 Alternate Hypothesis: 70% or more blockchain networks use decentralized identity management to improve trust in their networks (H1: p ≥ .70).

This hypothesis has been tested by using the acceptance of blockchain project managers, blockchain architects and blockchain consultants. It is seen that 82.75% of them have agreed to use decentralized identity management to improve trust in their blockchain networks as shown in Figure 4.

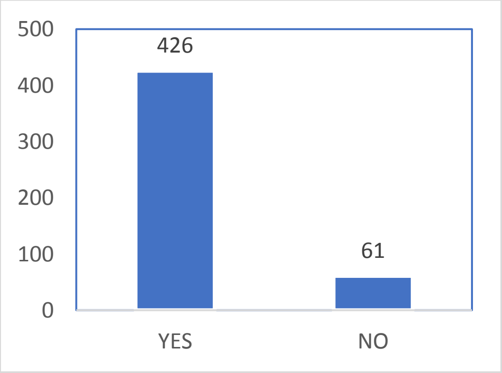

Figure 4: Use of DIM

χ2 value is found out to be 47.85 which is greater than the table value 3.84 at 5% level of significance. Hence, Null hypothesis is rejected and alternate hypothesis is accepted.

Table 1. Testing of hypotheses- Chi-square test results (N=487, df=1, α = 5% and χ2 =3.84)

Sr. No	Hypothesis	Chi-square (calculated)	Result
1	Does Layer 2 solutions enhance the capabilities of blockchain networks.	38.18	Ho rejected and H1 accepted
2	Does the overall security of blockchain networks be increased by upgrading the consensus mechanisms.	10.47	Ho rejected and H1 accepted
3	Can use of cross-chain bridges enable interoperability between different blockchain networks.	67.42	Ho rejected and H1 accepted
4	Does decentralized identity management has the potential to improve trust in blockchain networks.	47.85	Ho rejected and H1 accepted

V Conclusion

Blockchain technology has several advantages, including immutability, transparency, and security. However, it also has several problems that need to be addressed. This comprehensive review has highlighted some of the key problems associated with blockchain technology, including scalability, energy consumption, interoperability, regulatory challenges, and privacy concerns.

Scalability is a major issue in blockchain technology, as current blockchain systems are unable to handle the high volume of transactions required by mainstream adoption. Energy consumption is also a significant concern, as some blockchain networks consume large amounts of energy, which is not sustainable in the long term. Interoperability is another issue, as different blockchain networks often have different protocols, making it difficult to transfer value and data across networks. Regulatory challenges also pose a problem, as blockchain technology operates in a largely unregulated environment, and there is a need for greater clarity and consistency in regulations. Finally, privacy concerns exist around the use of public blockchains, which are not fully anonymous, and the potential for data breaches.

To address the above problems, various solutions have been proposed, including the use of sharding, proof of stake, and off-chain scaling solutions for scalability, the adoption of sustainable energy sources for energy consumption, the development of interoperability protocols and middleware solutions for interoperability, and the establishment of clear regulatory frameworks for regulatory challenges. Blockchain technology has the potential to revolutionize many industries, but there are several challenges that need to be addressed to enable its widespread adoption.

REFERENCES

[1] A. Saha, R. Amin, S. Kunal, S. Vollala, S.K. Dwivedi, Review on "Blockchain technology based medical healthcare system with privacy issues." Secur. Privacy 2(5), e83 (2019). https://doi.org/10.1002/spy2.83

[2] L. Ismail, M. Huned, Z. Sherali, in Lightweight Blockchain for Healthcare (IEEE, 2019), pp. 149935–149951. https://doi.org/10.1109/access.2019.2947613

[3] F. Tian, An Agri-Food Supply Chain Traceability System for China Based on RFID and Blockchain Technology (IEEE, Kunming, China, 2016)

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in 2017 IEEE international congress on big data (BigData congress) (IEEE, 2017), pp. 557–564

[5] A. Azaria, A. Ekblaw, T, Vieira, A, Lippman, in Medrec: Using Blockchain for Medical Data Access and Permission Management (IEEE, Vienna, Austria, 2016)

[6] Q. Xia, E. Sifah, A. Smahi, S. Amofa, X. Zhang, BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information 8(2), 44 (2017)

[7] A Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, F. Wang, Secure and trustable electronic medical records sharing using blockchain, in AMIA Annual Symposium Proceedings (Maryland, 2017)

[8] C. Esposito, A. De Santis, G. Tortora, H. Chang, K.K.R. Choo, Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 5(1), 31–37 (2018)

[9] A. Al Omar, M.S. Rahman, A. Basu, S. Kiyomoto, Medibchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data, vol. 10658 (Springer, Guangzhou, China, 2017)

[10] H. Kaur, M.A. Alam, R. Jameel, A.K. Mourya, V. Chang, A proposed solution and future direction for blockchain-

based heterogeneous medicare data in cloud environment. J Med Syst. 42(8), 156 (2018)

[11] Q. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access. 5, 14757–14767 (2017)

[12] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

[13] Vigna, P., & Casey, M. J. (2018). The truth machine: The blockchain and the future of everything. St. Martin's Press.

[14] Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104-113.

[15] De Filippi, P., & Loveluck, B. (2016). The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review, 5(3).

[16] Stinchcombe, M. B. (2017). An introduction to blockchain technology. IEEE Potentials, 36(2), 20-25.

[17] Zheng, Z., Xie, S., Dai, H. N., Chen, W., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 13(4), 352-375.

[18] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71-81.

[19] Swan, M. (2017). Blockchain thinking: The brain as a decentralized autonomous corporation. IEEE Technology and Society Magazine, 36(2), 41-52.