Enhancement of Blockchain, it’s Application, Challenges and Opportunities

Debajyoti Roy[1], Farhan Shamsad[2], Anirban Bhar[3], Suman Kumar Bhattacharyya[4]

[1,2] B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.
[3,4] Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

[1] roydebajyoti2002@gmail.com
[2] farhan.y2k.me@gmail.com
[3] anirban.bhar@nit.ac.in
[4] suman.bhattacharyya@nit.ac.in

ABSTRACT

In the present day and age, the Blockchain technology is growing more popularity with each passing day. This is since it has revolutionized the traditional commerce due to its distributed ledger feature. Additionally, every record in this ledger is secured by laws of cryptography, which makes it more secure and tamper-free. This, of course, resulted in the development of several distinct cryptocurrencies, such as Bitcoin, which is founded on a piece of technology that is more widely referred to as Blockchain. Due to the rapid advancement of Blockchain research, there is a need for additional research studies that investigate and analyze the present knowledge in this field through a methodical technical study that demonstrates the influence and significance of the relevant literature from the start of the technology in 2013. In order to accomplish what was set out to do, following the presentation of an unavoidable, condensed summary of Blockchain technology, the papers that were gathered were meticulously analyzed in accordance with seven primary research questions. After that, important and valuable findings, such as the top 10 influential papers, yearly publications and citation trends, the favorite publication venues, the hottest research areas, and the most supportive funding bodies are reported. These findings may offer several implications about the status quo as well as emerging trends and frontiers of Blockchain, and they are intended to guide towards the establishment of a baseline for both new and experienced researchers and practitioners prior to the beginning of a future research project. In conclusion, a quick overview of some ongoing difficulties and possible developments in the field of blockchain technology is provided.

Keywords: *Blockchain, Cryptography, Cryptocurrencies, Security.*

1. INTRODUCTION

A distributed and unchangeable data store that can be used in a wide variety of applications, such as electronic voting, crowdfunding, distributed resources, governing of public records, and identity management, is described as blockchain. Blockchain is roughly defined as an array of blocks that are individually connected to one another. Each block contains several transactions that yield the distributed and unchangeable data store. Following this, monetary transactions taking place between individuals or organisations are typically consolidated and managed by an independent firm. Within the context of information technology, blockchain makes it possible for technology to serve as the primary motivating factor behind the subsequent crucial revolution. The Internet of Things (IoT) and banking are only two examples of businesses that make considerable use of Blockchain technology implementations. Other examples include supply chain management, health care, and reputation management systems. Each application of Blockchain technology has its own unique advantages in these and other fields of endeavour. Enhancing manufacturing now requires the incorporation of online commercial transactions, information security, protection of personal privacy, and assurance of physical safety within an online environment. The increased utilisation of information and communication technology has contributed to the expansion of the economy. It is important to note that in 2016, only technology businesses and financial services providers invested more than one billion dollars in the deployment of blockchain technology. In addition to that, it is anticipated that the following few years would witness a significant growth in the total amount.

People now have access to an alternate, reliable third party to facilitate these kinds of online transactions thanks to the development of blockchain technology. Investigating various aspects of the Blockchain technology is essential because it encourages trust between peer-to-peer networks. This is achieved by the technology's considerations for security and privacy concerns within the context of the Internet environment for business-oriented individuals and organisations. The Blockchain technology has experienced fast expansion in recent years, which has left the academic community with a significant number of knowledge gaps to fill. As a direct consequence of this, the field of Blockchain has been the subject of a significant number of research projects in recent years. According to the procedure for collecting data that was utilised in this investigation, Web of Science (WoS) has been indexing more than 7000 scientific papers on its own during the past few years. As the number of publications in the Blockchain space continues to rise, in-depth research studies that investigate an overview of the existing body of related knowledge are required. In order to accomplish this goal, practitioners and researchers have been presented, through the use of a few review papers, with information regarding recent achievements and problems pertaining to Blockchain. However, there has not yet been published a comprehensive assessment of the literature that is based on WoS as a literature database and is comprised of the most recent scientific research that was carried out in the subject. Therefore, in order to keep making continuous development in this field, it is necessary to conduct an in-depth assessment of the current state of the art in the Blockchain domain in order to investigate this topic. The primary objective of this review is to provide the Blockchain community with another helpful guide. In addition, this study sheds intense light on some key new insights and future research directions beyond Bitcoin and cryptocurrencies regarding applications of Blockchain derived from previous studies addressed in this paper. It also sheds light on some current open issues and challenges, which opens up new avenues towards further future researches in the field. However, due to the fact that Blockchain technology is continuously advancing at an extremely rapid rate, we feel it is necessary to point you that our investigation cannot in any way be considered to be comprehensive.

2. PREVIOUS WORK

The phrase "cryptocurrency" is common in industry and academia. Bitcoin's capital market exceeded $10 billion in 2016 [1]. Bitcoin relies on blockchain, a 2008 proposal realised in 2009 [2]. A custom data storage structure could enable Bitcoin network transactions without third parties. A blockchain, or public ledger, records all committed transactions in blocks. As blocks are added, this chain grows. User security and ledger consistency are achieved through asymmetric cryptography and distributed consensus techniques. Blockchain technology requires decentralisation, persistency, anonymity, and auditability. Due to these traits, blockchain can cut costs and boost efficiency.

Blockchain allows direct payment without a bank or other middlemen, making it useful in digital assets, remittance, and online payment. [3], [4]. It can also be utilised in IoT, smart contracts, public services, reputation systems, and security services. These industries help blockchain in many ways. First, blockchain is immutable. Blockchain transactions cannot be changed. Companies that must be trustworthy and honest to attract customers can use blockchain. Due to its distributed nature, blockchain prevents single points of failure. Miners can automatically execute smart contracts on blockchains.

Blockchain technology has great potential for future Internet applications, but it must overcome technological challenges. First, scalability matters. Bitcoin blocks are currently 1 MB and mined every 10 minutes. Thus, the Bitcoin network can only execute 7 transactions per second, making high-frequency trading impossible. Larger blocks take up more storage and propagate slower over the network. Centralization will occur as fewer people maintain large blockchains. Thus, balancing block size and security is tough. Second, selfish mining can lead to unfair profits [10]. Miners hide extracted blocks to make more money. In that instance, many forks could hinder blockchain growth. Therefore, solutions must be presented to fix this. Even when users solely use their public and private keys for transactions, blockchain can leak privacy [11]. Current consensus methods like proof of work and proof of stake have many drawbacks. Proof of stake consensus may show that the rich become richer while proof of work wastes electricity.

Blockchain knowledge is available through blogs, wikis, forum posts, codes, conference papers, and journal publications. Tschorsch et al. studied Bitcoin's technical aspects [12]. We investigate blockchain technology, not virtual currency, unlike [12]. Blockchain was covered in a Nomura Research Institute technical report [13]. Unlike [13], our study covers cutting-edge blockchain research, including current and emerging trends.

3. BLOCK CHAIN OVERVIEW

Blockchain, in its most basic form, can be thought of as a distributed, digital public ledger in which all digital transactions are recorded as a series of blocks of data called "Completed Transactions" or in reverse chronological order.

Blockchain functions like a public ledger in that it records transactions in a continuously growing list of "blocks." These blocks are related to one another by the parent block's reference hash. A "Genesis block" is an initial building block that has no predecessors. The block header (80 bytes) of Bitcoin, one important instance of the Blockchain, contains metadata such as the block version (4 bytes), Merkle tree root hash (32 bytes), timestamp (4 bytes), nBits (4 bytes), nonce (4 bytes), and parent block hash (32 bytes).

Transactions, which are digital assets transmitted as a data structure between peers in a decentralized Blockchain network, are often initiated at a node using a digital signature based on private key cryptography. All transactions are stored in an unconfirmed transaction pool, and the Gossip protocol (a flooding mechanism) is utilized to spread them over the network. These transactions must then be selected and validated by peers based on a set of predetermined criteria.

Blockchain features include the elimination of the need for a centralized authority, such as a bank, to verify each transaction. Therefore, a decentralized P2P Blockchain architecture is necessary, with trust as the primary concern in decentralization, along with fail-over, availability, and increase resilience. In the Blockchain network, transactions between peers (P2P) don't require central authentication like they would in a centralized system.
Users can engage with a Blockchain without fear of their identities being revealed by having several, randomly generated addresses. Users' personal data is protected since no single entity is responsible for monitoring or storing it in a decentralized system. Since Blockchain operates in a trustless setting, it may be possible to maintain some degree of privacy when using it.

All three blockchain types may be demonstrated in their respective fields.
Transactions on a public blockchain are visible to all users of the network, and so is the procedure for reaching consensus. Public Blockchains include, but are not limited to, Bitcoin and Ethereum.
Private Blockchain: In this setup, the Blockchain is accessible to all nodes, but data access is strictly controlled by a central authority. Database management systems, Bankchain, Multichain, and Monax are just a few examples of private Blockchains.

Blockchain consortiums or federations combine public and private Blockchains into a single network. Additionally, it allows for a predetermined authorized node to be selected. In addition, B2B collaboration is commonplace. You can think of the data as being semi-decentralized as well. Hyperledger and the R3CEV consortium are two Blockchain examples.

4. METHODOLOGY AND APPLICATIONS

We begin by explaining why we decided to conduct this research. Second, we outline the procedures we took in order to find appropriate research. Both the initial list of articles and the inclusion and exclusion criteria used to get a filtered set of research are specified in great depth inside the methodology.

Find a relevant search engine - To meet our requirements, we first sought out a suitable search engine, and only then began to collect papers related to the Blockchain. WoS has been chosen as a data source for Blockchain studies out of the various current scholarly databases (such as Scopus, EBSCO, Google Scholar, etc.). Several factors contributed to the decision to use WoS as our primary citation index, including (i) its status as the first and world-leading citation index in the scientific community, (ii) its careful curation of high-quality and influential research publications, and (iii) its comprehensive coverage of more than 21,100 peer-reviewed, high-quality scholarly journals (including Open Access journals), books, and conference proceedings published worldwide.
We used a search query string that included phrases like "Blockchain," "cryptocurrency," "Bitcoin," "Ethereum," and "smart contract" to retrieve the relevant publications. There has been a constant increase in the number of Bitcoin-related publications since Nakamoto's paper appeared in 2008 (Nakamoto,2008). However, there has been a dramatic shift in publication patterns from 2016 to 2020, as scholars have shifted their focus from other areas of study to Blockchain.

The application and feature include

4.1 Business and industrial applications

Through the automation, improvement, and optimization of business processes, Blockchain has the potential to be a game-changing innovation driver in business and management. In the realm of e-commerce, many IoT-blockchain-based concepts are now in development. Business models based on the usage of smart contracts stored in a distributed database like Blockchain have been presented, such as the one put forth by Zhang and Wen (2017). A Blockchain-based Internet of Things (IoT) network was presented in Hardjono et al. (2016) as a privacy-preserving solution to confirm provenance manufacturing in the absence of third-party verification. Furthermore, it has become evident that Blockchain applications present commercialization potential and substantial enhancement in the overall performance, allowing IoT businesses to optimize their operations and bolstering the legitimacy of e-commerce while saving time and money. Furthermore, many businesses may benefit from using Blockchain-based applications as their business process management solutions. Each instance of a business process could then be stored in the Blockchain, and smart contracts could be utilized to accomplish the workflow routing, all while minimizing overhead and increasing productivity within an organization.

4.2 Financial applications

Economic transactions, prediction markets, the settlement of financial assets, business services, and the finance industry all make heavy use of Blockchain technology right now. Consumers and the established financial system alike stand to benefit from the widespread adoption of blockchain technology, which is predicted to play a significant role in the long-term growth of economies around the world. Due to the lack of official backing, cryptocurrencies have less value and less price stability than traditional fiat currencies. Blockchain encrypted cryptocurrencies, however, offer a fast and cheap means of trade. It's important to note that Bitcoin is just one example of many different cryptocurrencies that have been developed and put into use. It's important to note that the cryptocurrency's worth is expressed in terms of fiat currency. The following pursuit of Blockchain-enabled applications on financial assets (such as derivative contracts, fiat money, securities, etc.) by the global financial system is not surprising.

4.3 Education

Blockchain was developed for use in trustless monetary transactions; but, if we think of the learning process as currency, we may apply it to the online education sector. Thus, Blockchain learning arose, wherein educators could cram and deposit blocks into Blockchain, treating student accomplishments as currency. Thus, in the context of pervasive learning environments, Blockchain can be used to store educational records of reputation awards based on a distributed system, as well as to address privacy, security, and vulnerability concerns. Credit management and the maintenance of educational certificates can both benefit from Blockchain's increased trustworthiness and data security in digital infrastructures. In addition, using applications built on the Blockchain could improve digitally accredited academic and individual learning. To better gather, report, and analyses data regarding school systems for decision making, Blockchain-based school information hubs could be set up. Finally, Blockchain can be utilized in scholarly publication to improve the handling of a manuscript submission by authenticating the article itself and making every effort to conduct relevant reviews immediately.

4.4 Governance

By fostering a more open relationship between the government and its citizens, blockchain technology can help governments enhance the services they provide. To reduce tax evasion and improve government services, waste and red tape must be reduced. Over the years, residents and businesses have committed their official records to the care of their respective governments. Blockchain-based apps may alter the way city or state governments function through transaction disintermediation and record-keeping. Blockchain technology has the potential to improve government efficiency by preventing corruption through its secure, automated, decentralized, and accountable handling of public records. In a smart city setting, in particular, Blockchain might be adopted as a secure communication platform and used to facilitate the integration of corporate, social, and physical infrastructures. Blockchain governance's ultimate goal is to efficiently and decentralizedly supply the same services supplied by the state and its public authorities. Voting, taxation, marriage licenses, personal identity, notarization, and registration or legal documentation are all examples of such services.

4.5 Security and Privacy

It has been proposed that Blockchain's privacy concerns can be addressed by establishing and maintaining digital identities within the bounds of a regulatory framework that allows for the widespread adoption of the Blockchain model while protecting users' right to anonymity in matters of ownership and control. As more and more people use smartphones and related services, there will inevitably be more opportunities for bad actors to exploit security flaws. Several anti-malware filters are proposed to keep and update the virus patterns on a central server, allowing for the detection of dubious files based on pattern-matching algorithms. However, these centralized defenses are within the reach of hostile attackers. Therefore, Blockchain technology can greatly enhance the safety of decentralized systems. In one paper in particular, BitAV, a unique anti-malware environment in which Blockchain users disseminate pathogen patterns, was proposed. This is another method in which BitAV increases fault tolerance.

The number of blockchain-based applications is growing rapidly, but there are still difficulties with interoperability and standardization. Integrating blockchain technology with SC improves product authenticity, security, traceability, management, and transparency across the supply chain as a whole, while also cutting down on paperwork and human error. The question of whether or whether blockchain systems ought to be standardized and compatible with one another, however, merits additional investigation.

Despite the many potential advantages, widespread implementation is hampered by internal and external organizational challenges. Organizational preparedness, technical know-how, digital infrastructure, scalability issues, financial resources, legal and regulatory compliance, organizational resistance, performance expectations, standardization, model security, and country of business are just some of the many factors that affect adoption. It is becoming increasingly important to involve government agencies for rules and regulation compliance while building new blockchain-based solutions, as local and national regulations frequently constitute an impediment to blockchain breakthroughs. Since both customers and workers will need to adjust their purchasing and operational habits, education and empowerment of the former are crucial to the latter. When it comes to expanding blockchain's reach and coverage, the least investigated topics are organizational preparedness and legislation. Remember that there is no way to avoid dealing with the law and regulations in company. More work is needed to understand how best to apply smart contracting systems in logistics while addressing all of these concerns. Therefore, this should be taken into consideration while developing blockchain platforms for efficient smart contract execution. Organizational unwillingness to exchange data on a global scale remains a significant barrier. Challenges to scaling up, such as a lack of common standards across multiple organizations, could cause interoperability problems. A unified norm for addressing the problem requires cooperation between the government and the business community.

While blockchain is widely recognized as a tamper-proofed data storage architecture and one of the best-secured transaction platforms, it does not come without its fair share of technical challenges. The following is a synopsis of some of the technical challenges that typically arise when conducting SC operations that make use of blockchain technology.

Several major scalability issues might occur with blockchain technology, as the number of transactions continues to grow: chain limits, big block sizes, delayed response times, and excessive fees. The increasing number of daily users is compounding the problems of scaling the blockchain.

Data confidentiality and privacy are still problems with blockchains, despite the fact that they are integral parts of data management. This is especially relevant to the public blockchain, which acts as a public ledger yet holds data and various privacy-related properties.

Key elements of interoperable blockchain designs include the sharing of data between blockchains in order to facilitate different types of block transactions or the use of data by different blockchain implementations. As the number of blockchain apps proliferates, so does the importance of the interoperability problem.

Provenance, or the background, roots, and origins of a product, is an integral part of blockchain technology. It is critical to have a firm grasp on how to effectively relay information about the product's origins.

Latency: The Bitcoin block processing time, transaction rate, and security check all take several minutes, suggesting that blockchain infrastructures will face substantial latency difficulties.

Auditing, transparency, and disintermediation are also crucial components of blockchain technology. To guarantee smooth and trustworthy transactions, these features must be strictly monitored to assure error-free verification and auditability, straightforward tracking, and the absence of any third-party mediation.

Traditional problems in SC operations and logistics management, such as raw material and product damage, erroneous data input, order mishandling, etc., persist. Several parties, such as international logistics partners, operational efficiency, maintenance costs, large data management, and IT support, would need to work together for blockchain to be adopted and run efficiently in SC.systems. Government regulations on cryptocurrencies, data warehousing, scalability, and high-speed internet access with vast computer capacity are all examples of difficulties that need solving. Inadequate infrastructure and the aforementioned constraints may make it impossible for every node in the blockchain to process and confirm every transaction, which can be a problem in both developed and developing countries. Adaptability, standardization, scalability, and synergy amongst different technologies are other important questions to ask. In order to examine the various facets of adoption, a unifying theory of acceptance and usage of technology has been created in the literature.

5. FUTURE SCOPE

Blockchain technology has the potential to revolutionize the financial industry by simplifying and automating processes, lowering transaction costs, and boosting trust and transparency. The efficiency of capital markets can be enhanced, new financial goods and services developed, and payment systems facilitated at lower cost thanks to its application.

Blockchain technology can be used in supply chain management to verify the authenticity and legitimacy of products and services as they make their way from point A to point B. Food fraud can be reduced, food safety can be enhanced, and sustainability can be promoted.

Blockchain has applications in healthcare, including the safekeeping and distribution of medical records, the protection of patient confidentiality, and the facilitation of clinical trials. It can also be applied to the creation of innovative medical technologies like telemedicine and online drugstores.

Government: Blockchain can be used to make services like voting, land registration, and tax collecting more secure and transparent. It can also be utilized to develop innovative public programmes, such as digital identity and social welfare services.

Blockchain technology might also have a profound impact on industries as diverse as the ones dealing with energy, real estate, and the arts. It has several potential applications, including the creation of decentralized social media networks, the defense of intellectual property, and the development of new energy markets.

In addition to the aforementioned prospects, blockchain technology may potentially give rise to whole new markets and businesses that do not now exist. We can anticipate many more cutting-edge uses of blockchain technology as the technology evolves and advances.

6. CONCLUSION

In summary, blockchain technology stands as a disruptive force with the potential to redefine industries and reshape our digital future. Its decentralized and transparent ledger system offers opportunities for innovation across sectors such as finance, healthcare, and supply chain management. Blockchain's core attributes, including immutability and enhanced security, are driving its adoption.

Nevertheless, challenges persist. Scalability issues need resolution to support widespread use, and regulatory frameworks require careful development to balance innovation and security. Interoperability between various blockchain platforms remains a critical concern, demanding the creation of industry standards.

Collaboration is paramount for success. Governments, industries, and the blockchain community must work together to overcome these challenges. With continued research and development, blockchain technology can unlock its full potential, fundamentally altering how transactions are conducted, data is secured, and innovation is catalyzed in our rapidly evolving digital landscape. Its promise in enhancing security, transparency, and innovation makes it a potent tool for shaping the future of multiple sectors and society at large.

6. REFERENCES

[1]. “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016.
[2]. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[3]. G. W. Peters, E. Panayi, and A. Chapelle, “Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective,” 2015.
[5]. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
[6]. B. W. Akins, J. L. Chapman, and J. M. Gordon, “A whole new world: Income tax considerations of the bitcoin economy,” 2013.
[7]. Y. Zhang and J. Wen, “An iot electric business model based on the protocol of bitcoin,” in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.
[8]. M. Sharples and J. Domingue, “The blockchain and kudos: A distributed system for educational record, reputation and reward,” in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.
[9]. C. Noyes, “Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning,” arXiv preprint arXiv:1601.01405, 2016.
[10]. I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436– 454.
[11]. A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin p2p network,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.
[12]. F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Sur- veys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.
[13]. NRI, “Survey on blockchain technologies and related services,” Tech. Rep., 2015.