A Review Paper on Blockchain Technology

Sweta Kumari Barnwal, Assistant Professor

Department of Computer Science, Arka Jain University, Jamshedpur, Jharkhand, India

Email Id- sweta.b@arkajainuniversity.ac.in

ABSTRACT: From a technical perspective, Blockchain produces interesting research subjects since it enables security, anonymity, and data integrity without a third-party organization regulating transactions. Blockchain is a decentralized transaction and data management system that was first developed for the Bitcoin cryptocurrency and is now utilized by a wide range of businesses. We will emphasize the applications and contributions of blockchain technology in finance in general, as well as areas where the technology may have a greater effect on payment systems, in this article. The authors examine the successful applications of blockchain technology in a variety of financial areas, including cryptocurrency, in addition to giving a thorough study of blockchain technology and cryptocurrencies. The authors carefully evaluate technical research on bitcoin price behavior. Crypto currency, which is the first successful application of blockchain technology, may fuel a money transfer network.

KEYWORDS: Blockchain, Cryptocurrency, Network, Security, Technology.

1. INTRODUCTION

People and businesses often use the help of a third-party organization to oversee their money transactions. A bank or credit card issuer must act as an intermediary in order to complete a digital payment or currency transfer. A bank or credit card issuer for a transaction charges an extra fee. This process affects other areas, such as video games, music, and software. Rather than the two primary parties involved in the transaction, all data and information is managed and kept by an independent third-party organization. Blockchain technology was developed to address this issue, and it is already in use. Blockchain technology was created as a way to create a decentralized ecosystem where no third party controls transactions and data [1].

Block-chain is a distributed database that keeps track of an ever-growing list of data entries that are validated by the network's nodes. Every transaction is recorded on a public ledger. A third-party intermediary is no longer required thanks to decentralized blockchain technology. Every node in the blockchain network has access to data on every transaction that has ever occurred. Compared to centralise transactions involving a third party, this feature improves transparency. Because the nodes in Blockchain are anonymous, it is safer for other nodes to validate transactions. It was a game-changer when Blockchain technology was first utilized in Bitcoin. Because of the decentralized environment it provides, participants may buy and sell items using digital money [2].

1.1 Overview Of Blockchain Technology:

Decentralized currencies, self-executing contracts (smart contracts), and intelligent assets that can be controlled via the Internet are all possible with blockchain technology (smart property). Decentralized (autonomous) organisations that may function across a network of computers without any human involvement are also possible using blockchain. With these uses, some have drawn comparisons between Blockchain and Internet, predicting that it would help displace centralised authority in the fields of communications, economic transactions, and even politics or law [3].

Prior to the development of the blockchain, it was difficult to coordinate individual activities via the Internet without a centralised authority to guarantee that the data was not changed with. A group of unconnected people could not confirm that an event had occurred without a central authority to check that the transaction was neither fraudulent nor invalid. When there was no central clearinghouse for the dispersed gathering of people, it was believed that unanimity was unattainable [4]. A probabilistic approach utilizing a blockchain may be used to address this issue. It makes information flowing across a network of computers more visible and verifiable while dealing with computationally demanding mathematical issues. It will be more difficult for an attacker to harm a shared database with false information if they do not control a majority of the network's processing capacity. Because blockchain protocols guarantee that transactions on a blockchain are legal and never recorded to the common repository more than once, decentralized transactions may be coordinated without relying on a trusted third party to verify and clear all transactions [5].

1.2 Emerging Uses Of Blockchain Technology:

Cryptographic tokens that might represent property or ownership interest in future services have been created by software developers who have swiftly grasped the possibilities of blockchain technology. Decentralized domain name management systems (DNS) and censorship-resistant digital voting platforms are also being developed with it. For this reason, the technology is becoming recognised as a means to facilitate machine-to machine connections that will soon arise from the Internet of Things' Internet-enabled objects. This is because the blockchain combines digital currency, smart contracts, and distributed data storage to create completely new decentralised organisations (such as autonomous decentralised organisations) that utilise source code to design a governance structure for their companies [6].

1.3 Digital Currencies and Global Payment Systems:

Digital currencies such as Bitcoin were one of the first implementations of blockchain technology. From the anonymous organisation or individual known only as Satoshi Nakamoto, this book was published in 2009. This digital money, unlike the US dollar, does not depend on any bank or government. As Nakamoto explains, the system is "totally decentralised, with no central server or trusted parties, because everything is based on crypto evidence instead of trust".

From the moment it was first introduced, Bitcoin has captivated the interest of the globe. However, Bitcoin is utilised for more than simply speculative purposes nowadays. A completely new payment system is powered by it, allowing for frictionless transfers of cash throughout the world. A bitcoin transaction may be transmitted around the globe in less than seven minute, compared to days for conventional payment methods such as Western Union. Only an Internet connection and a computer or mobile device are required [7].

Cryptocurrencies like Bitcoin have been gaining popularity rapidly, and they have the potential to be the first breakthrough applications that rely on blockchain technology. Athey notes that these digital currencies have the ability to boost international trade, support financial inclusion and alter the way we spend money, save money and do business in ways we haven't completely grasped as of yet." There is a potential for faster and cheaper bank transfers, the expansion of banking and e-commerce operations to third-world nations, and a significant reduction in merchant fraud if this technology is implemented [8].

1.4 Ethereum:

A blockchain-based virtual machine and Cloud 2.0 platform, Ethereum has stateful user-created digital contracts that may be executed in real time. The engineers are working on a system that will allow for the exchange of complicated contracts, which will be available in the future. As users become more sophisticated in their interactions, they will be able to enter into digital contracts using a distributed ledger architecture [9]. Crypto-economy is being extended beyond virtual currency transactions with Ethereum, which provides a strong technological and legal foundation for the development of a nexus of digital contracts related to all sectors of life (for example, wage payment or marriage).

1.5 Distributed and Secure Data Stores:

A decentralised, encrypted database, blockchains are also beginning to influence the way we communicate and exchange data online because of their decentralised nature. Additionally, they are increasingly regarded as a means to promote machine-to-machine connections for Internet enabled devices. Blockchain technology eliminates the need to route conversations and data through a centralised system or internet platform (like Gmail for e-mails or Dropbox for the exchange of digital files). Parties can save and retrieve communications without the danger of government intrusion using decentralised, encrypted communication protocols and a blockchain. The same technology also enables for the decentralised and safe sharing of data. Publication and distribution of information over hundreds of thousands of computers (encrypted if required) makes censorship nearly impossible. People are encouraged to use their spare hard drive space by using anonymous, decentralised cloud storage solutions that employ blockchain technology and other peer-to-peer technologies [10]. A number of technical problems and constraints associated with blockchain technology have been discovered. In the future, blockchain technology will face seven technological problems and limitations:

Throughput: The Bitcoin network's maximum throughput is presently 7tps (transactions per second). VISA (2,000tps) and Twitter are two other transaction-processing networks (5,000tps). In order to maintain the same level of transaction frequency, the blockchain network's throughput must be increased. Latency: Currently, it takes about 10 minutes to complete a transaction in order to ensure the security of a Bitcoin transaction block. Because double spending assaults are costly, more time must be spent on a block to achieve efficiency. As a result, latency is now a major problem in the blockchain world. As long as security is maintained, it should be

possible to create a block and confirm the transaction in a few seconds. To execute a transaction with VISA, for example, it takes only a few moments.

Size and bandwidth: Bitcoin's blockchains are over 50,000MB in size at now (February 2016). 214PB per year might be added to the blockchain if throughput reaches VISA levels. It is assumed by the Bitcoin community that one block is 1MB in size with one block being generated every 10 minutes. It follows thus that transactions are limited in quantity (on average, 500 per block). To increase the number of transactions that the blockchain can handle, the size and bandwidth concerns must be addressed first.

1.5.1 Security:

The present Blockchain is vulnerable to a 50 percent assault because of the way it is designed. The bulk of the network's mining hash-rate would be under the control of a single organisation, allowing it to influence Blockchain. Additional security research is required to solve this problem.

1.5.2 Resources that have been wasted:

Bitcoin wastes Mining in the billions of dollars a day. Cryptocurrency's Proof-of-Work effort is to blame for wasting Bitcoin's resources. A miner's Bitcoin holdings are used to compare resources while using Proof-of-Stake. When someone holds 1 percent of bitcoin, they may mine 1 percent of the blocks that prove their stake. In order to improve the efficiency of mining in Blockchain, the problem of wasted resources must be addressed and resolved.

1.5.3 User-friendliness:

The Bitcoin API for creating services is not very user-friendly. For Blockchain, a more developer-friendly API is required. REST APIs are a good example of this.

It is all there: versioning, hard forks, and numerous chains of code 51 percent attacks are more likely to occur in chains with a small number of nodes. When chains are separated for administrative or versioning purposes, another difficulty arises.

1.6 Decentralized (Autonomous) Organization:

As a result, Michael Jensen and William Meckling's notion that entities are nothing more than a collection of contracts and connections is now a reality. As the world's first decentralised public ledger, Bitcoin has grown in popularity since 2013-2014. Despite the fact that mainstream adoption is still a long way off, the success of Bitcoin may be attributed to the underlying technology known as the blockchain. An electronic public ledger platform that is shared by all participants through the Internet or another distributed network of computers. As a rule, blockchain is designed to eliminate the requirement for a trusted third party to ensure transactions, with the noteworthy exception of token-free applications we will go through five of the most essential characteristics of public ledgers in the following paragraphs.

However, even while Blockchain appears to be a good option for conducting transactions using cryptocurrencies, it still has certain technological problems and limits that need to be explored and dealt with in the future. To avoid assaults and efforts to disrupt transactions in Blockchain, high integrity of transactions and security, as well as privacy of nodes, are required. Aside from that, verifying transactions in the Blockchain needs a lot of computing power. What subjects have already been investigated and handled in Blockchain, as well as what are the current major problems and limits that require additional study, are crucial to recognise and understand. A thorough mapping study approach was used in order to find relevant Blockchain-related articles. A well-designed procedure was used to scan scientific databases in the systematic mapping investigation. Researchers and practitioners will be able to discover prospective study areas and issues for future research thanks to the map of existing research on Blockchain.

1.7 Challenges Faced By Blockchain Technology:

Almost everyone would agree that the blockchain technology has the ability to fundamentally alter society, and notably banking and economics, in the near term. On its road to becoming a key ecosystem for the global financial network, this cutting-edge technology must overcome a number of challenges. Numerous reasons hinder cryptocurrencies and blockchain technology from becoming a global standard for financial transactions, despite its many benefits. In the absence of rules, users are concerned. Legal status as a means of making a long-term payment system Standardizing market components and reducing volatility will be achieved through legislation.

The use of cryptocurrencies in money laundering and financial crimes, as well as its usage by the black market, is another significant concern connected to the absence of laws. In addition, users may enjoy the maximum level of anonymity because to the nature of the blockchain network's architecture. While criminals and drug dealers may now disguise their identities while accessing blockchains and committing crimes using cryptocurrency, it has also provided criminals and drug dealer's new chances. For this reason, legal reforms are urgently needed to prevent such crimes from taking place in the first place.

Blockchains innovative technology makes it a popular alternative to conventional systems for money transfers and record keeping, but it is still at risk of being attacked by hackers. No recent cryptocurrency-related hacking instances used blockchain technology, but rather digital currency exchanges. Cryptocurrency's network security has never been hacked by hackers. Each exchange is responsible for implementing and maintaining the security protocol used at digital currency exchanges. However, these hacking stories have a detrimental impact on users' and prospective users' perspectives. There is no doubt about it, but news about hacking incidents at exchanges has generated a bad image of cryptocurrencies and blockchain that has yet to be overcome.

1.8 Public Ledgers under Criticism: Toward Hybrid Solutions?

Technological advances have always provided a means of shifting power from central authority to the populace. A few centuries ago, early mechanical advances permitted individuals to track their own time in the same manner that massive and expensive clock towers were a testament to the concentration of power in the hands of a minority. Traditional banking's basic concepts are at odds with the blockchain. An accountant's propensity is to consolidate all payment, transaction, and loan information in a computer system. This is what a banker's job is all about: keeping money and money information. It is possible that blockchain technology will be a game changer for the financial sector as a whole. Reviewing possible applications that might increase the efficiency of financial organisations while reducing their costs

We look at the advantages and disadvantages of this emerging decentralised technology, arguing that widespread adoption will lead to the expansion of a new subset of law known as Lex Cryptographia: rules administered through self-executing smart contracts and decentralized (autonomous) organizations. Governments and large multinational corporations may lose their ability to control and influence the behavior of diverse people through traditional means because of the widespread usage of blockchain technology. This implies that a deeper knowledge of how to regulate blockchain technology and how to lead the creation and deployment of these new decentralized organizations in ways that have not previously been addressed under current legal theory will become more important.

2. DISCUSSION

Cryptocurrencies such as Bitcoin and Ethereum have the potential to change our societies in profound ways. In order to avoid utopian aspirations and the traps of technocratic thinking and predestination, the risks and advantages of its prospective uses must, nevertheless, be carefully balanced. Allowing the decentralisation of government services through permissioned blockchain is both practical and desired, since it can improve the efficiency of government services. In contrast, the dangers and downsides of decentralisation of governance through open, distributed blockchains, such as Bitcoin, outweigh the benefits. In addition to a large number of third parties and successful companies offering intermediation services, fully distributed blockchain ecosystems are characterised by severe information and power imbalances between developers and consumers.

Concentration of power in the hands of key engineers and a lack of openness in decision making due to all of these reasons, existing distributed networks' egalitarian character is called into doubt, rendering some blockchain proponents' hopes unrealistic. It turns out that the concept of a blockchain-based authority is misleading, since authority is actually more subtle. There are hence reasons to question the role of the blockchain-based governance as a great facilitator of individual power, in an absolute sense. Due to the prominent role of markets and the speculative verification methods of fully distributed blockchains, the promise of empowering individuals is likely to remain unfulfilled. Yet another nefarious development may be hidden behind the process of devaluing public institutions, giving precedence to economics over politics, and transforming citizens into customers with the promise of more freedom and efficiency, as well as greater equality. In fact, this type of power transfer has been going on for decades, in many forms, with tremendous social and economic costs attached to it.

Antipolitical forces are capable of undermining the exact democratic principles that libertarians today fight to protect. The fact that overthrowing the State and absorbing its functions is a profitable business cannot be overlooked when evaluating the risks and benefits of blockchain applications. While the blockchain was originally created to eliminate the need for a third party in transactions, stakeholders now involved in blockchain governance play the classical role of tertius gaudens. in which the state is replaced in some or all of its functions

by a third party; even worse, these agents may deliberately pursue a divide and imperia strategy between civil society and the state in order to undermine traditional democratic order, modify existing power balances, and gain dominance in society. Anyhow, certain associates may accumulate enough wealth to form an authoritarian regime." A decentralised algorithm-based society is a realistic assumption if the neo-liberal ascendancy and its corporate goal produce its own brand of democracy.

3. CONCLUSION

Most techno-libertarians believe that the block chain's ability to establish consensus between participants on a wide scale is particularly important since they believe that centralised vertical authority is harmful to individual powers. It is not uncommon for them to espouse a utopian vision of a non-hierarchical, non-coercive society controlled by algorithm-based consensus, in which individuals may freely interact. A variety of additional ICT clichés has arisen in recent decades, such as "the myth of a better government" and "the idea of a perceptive and empowered customer." Briefly, we will look at reasons why blockchain governance does not solve either the political problem of compulsion, or the social problem of hierarchical organisations. According to a logical conclusion, blockchain-based governance should be considered an organisational theory with major technical and administrative benefits for markets, private services, and communities, rather than a political theory in and of itself.

A similar distinction may be made about the use of blockchain technology and decentralised platforms as pre-political instruments. Otherwise, blockchain-based governance might be viewed as amoral anti-politics wrapped up in language of inevitability when it comes to globalization's operation the free-market. As global civil society explores new political and social dimensions, the challenge will be to integrate disruptive technology like blockchain with citizens' rights, equality, social cohesion, inclusion and public sector protection. A mature and multidisciplinary endeavour by all disciplines of human knowledge, with special attention to political theory, humanities, and social sciences, is required to better assess risks, advantages, and consequences of new technology.

REFERENCES

[1] P. S. M. K. Alex Kibet, "A Synopsis of Blockchain Technology," *Int. J. Adv. Res. Comput. Eng. Technol.*, 2018.

[2] B. K. Mohanta and D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)," *2018 9th Int. Conf. Comput. Commun. Netw. Technol.*, 2018.

[3] R. Srivastava, S. Kumar, and A. S. | H. M. Saraswat, "Blockchain : A Revolutionary Technology," *Int. J. Trend Sci. Res. Dev.*, 2018, doi: 10.31142/ijtsrd12751.

[4] D. M. Kayam, "Blockchain Technology: An Approaching Game Changer in Financial Service Industry," *Int. J. Trend Sci. Res. Dev.*, 2018, doi: 10.31142/ijtsrd15928.

[5] N. Rifi, N. Agoulmine, N. Chendeb Taher, and E. Rachkidi, "Blockchain Technology: Is It a Good Candidate for Securing IoT Sensitive Medical Data?," *Wirel. Commun. Mob. Comput.*, 2018, doi: 10.1155/2018/9763937.

[6] P. R. Newswire, "Global Blockchain Technology Industry," *NY-Reportlinker*, 2018.

[7] Z. Allam, "On Smart Contracts and Organisational Performance: A Review of Smart Contracts through the Blockchain Technology," *Rev. Econ. Bus. Stud.*, 2018, doi: 10.1515/rebs-2018-0079.

[8] T. Thurner, "Supply chain finance and blockchain technology – the case of reverse securitisation," *foresight*, 2018, doi: 10.1108/fs-08-2018-099.

[9] L. C. Arcos, "The blockchain technology on the music industry," *Brazilian J. Oper. Prod. Manag.*, 2018, doi: 10.14488/bjopm.2018.v15.n3.a11.

[10] A Tilooby, "The Impact of Blockchain Technology on Financial Transactions," *August 14*, 2018.