IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12218

An Analysis of blockchain technology

Yogendra Kushwaha[1], Awadhesh Kumar Maurya[2], Kalpana[3]

Guest Faculty, Department of Computer Science & Engineering, MCAET, Ambedkar Nagar U.P., India [1]

Assistant Professor, Department of Information Technology, IET, DR. RML Avadh University, Ayodhya U.P., India [2]

Assistant Professor, Department of Agriculture (Crop Physiology), ABBSM Pura Bazar, Ayodhya U.P., India [3]

Abstract: From a technological standpoint, Blockchain creates intriguing study topics since it allows for confidentiality, anonymity, and data integrity without the need for a third party to oversee transactions. A large number of companies now use blockchain, a decentralised transaction and data management system that were initially created for the Bitcoin cryptocurrency. In this article, we'll focus on the uses and contributions of blockchain technology in finance generally, as well as on places where the technology might have a bigger impact on payment systems. In addition to providing a complete analysis of blockchain technology and cryptocurrencies, the authors look at the successful uses of blockchain technology in a number of financial sectors, including cryptocurrency. The technical studies on the price behaviour of bitcoin are carefully examined by the authors. As the first effective implementation of a blockchain, cryptocurrencies.

Keywords: Blockchain, Integrity, Confidentiality, Anonymity Cryptocurrency, Technology.

I. INTRODUCTION

People and companies frequently use the assistance of a third-party firm to monitor their financial transactions. A digital payment or currency transfer cannot be completed without the assistance of a bank or credit card issuer. A bank or credit card company may impose an additional fee for a transaction. Other fields including software, music, and video games are impacted by this process. All data and information are controlled and retained by an impartial third-party organisation rather than the two main parties involved in the transaction. This problem was addressed by the creation of blockchain technology, which is already in use. In order to build a decentralised ecosystem where no third-party controls transactions and data, blockchain technology was developed [l].

A distributed database called a blockchain keeps track of a rising number of data entries that are verified by network nodes. A public ledger keeps track of every transaction. The decentralised nature of blockchain technology eliminates the need for an intermediary third party. In the blockchain network, every node has access to information about every transaction that has ever taken place. This feature increases transparency when compared to centralising third-party transactional activities. It is safer for other nodes to validate transactions because the nodes in Blockchain are anonymous. The introduction of Blockchain technology in Bitcoin was a game-changer. Participants are able to purchase and sell products using digital money because of the decentralised environment it offers [2].

1.1 An orientation to blockchain technology

Blockchain technology makes it feasible for decentralised currencies, smart contracts that execute themselves, and internet-controllable intelligent assets (smart property). Blockchain technology also makes it feasible for decentralised (autonomous) organisations to run entirely autonomously over a network of computers. With these applications, some have compared Blockchain to the Internet and predicted that it would help usher in a time when centralised authority would be less important in the areas of communication, commerce, and even politics or the law [3].

Without a centralised authority to ensure that the data was not modified, it was challenging to coordinate individual activities via the Internet before the blockchain was developed. Without a centralised body to ensure that the transaction was legitimate and neither fraudulent nor invalid, a collection of unrelated individuals could not validate that an event had occurred. Unanimity was thought to be impossible since there was no central clearinghouse for the dispersed crowd [4]. This problem might be solved using a probabilistic method and a blockchain. While addressing computationally challenging mathematical problems, it increases the visibility and verifiability of information moving over a network of computers. If an attacker does not own a significant portion of the network's computing power, it will be more challenging for them to compromise a shared database with fake information. Decentralized transactions can be coordinated without relying on a trusted third party to validate and clear all transactions since blockchain protocols ensure that transactions on a blockchain are legitimate and never recorded to the common repository more than once [5].

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12218

1.2 New Applications for Blockchain Technology

Software developers who have quickly grasped the potential of blockchain technology have designed cryptographic coins that could possibly represent real estate or ownership stake in future services. It is also being used to create censorship-resistant digital voting platforms and stateless domain name systems (DNS). Because of this, the technology is starting to be acknowledged as a way to support the machine-to-machine communications that will inevitably result from the Internet of Things' items that are Internet-enabled. This is because to the blockchain's ability to integrate distributed data storage, smart contracts, and digital money to produce entirely new types of complex organizations (such autonomous complex organizations), which employ source code to construct a governance structure for their businesses [6].

1.3 Global Payment Systems and Digital Currencies:

One of the earliest uses of blockchain technology were digital currencies like Bitcoin. This book, written by the unnamed entity or person known only as Satoshi Nakamoto, was released in 2009. Unlike the US dollar, this digital currency is not backed by any bank or authority. Because everything is based on crypto proof rather than on confidence, the system is "completely decentralised, with no central server or trusted parties," according to Nakamoto.

The world has been fascinated by Bitcoin ever since it was originally introduced. Nowadays, though, Bitcoin is used for more than just speculation. It powers a brand-new payment system that makes it possible to send money anywhere in the world without any hassle. Compared to days for traditional payment channels like Western Union, a bitcoin transaction may travel the world in less than seven minutes. The only prerequisites are a PC or mobile device with an Internet connection [7].

Bitcoin and other cryptocurrencies are growing in popularity quickly and may prove to be the first ground-breaking uses of blockchain technology. They point out that these digital currencies have the potential to expand global trade, promote financial inclusion, and change how we spend, save, and do business in ways we haven't fully understood yet. " If this technology is used, there is the potential for quicker and more affordable bank transfers, the expansion of banking and e-commerce operations to developing countries, and a considerable decrease in merchant fraud [8].

1.4 Ethereum:

Ethereum is a blockchain-based virtual machine and Cloud 2.0 platform that allows for the instant execution of stateful user-generated digital contracts. Future systems that will enable the exchange of complex contracts are now being developed by the engineers. Users will be able to sign digital contracts utilising a distributed ledger architecture as their interactions become more sophisticated [9]. With Ethereum, which offers a solid technological and legal foundation for the establishment of a nexus of digital contracts relevant to all domains of life, the crypto economy is being expanded beyond virtual money transactions (for example, wage payment or marriage).

1.5 Secure and distributed data stores:

Blockchains are a decentralised, encrypted database that are starting to have an impact on how we communicate and exchange data online. They are also being viewed more and more as a way to encourage machine-to-machine connections for Internet-enabled devices. The requirement to pass communications and data through a centralised system or online platform is eliminated by blockchain technology.Using decentralised, encrypted communication protocols and a blockchain, parties can store and retrieve communications without worrying about governmental eavesdropping. The same technology makes it possible for data to be shared securely and decentralised. Censorship is practically impossible due to the publication and distribution of information over hundreds of thousands of computers (if necessary, encrypted). Utilizing anonymous, decentralised cloud storage services that make use of blockchain technology and other peer-to-peer technologies encourages people to make use of their unused hard drive space [10]. There have been shown to be some technical issues and limitations with blockchain technology. Future blockchain technology will encounter the following seven technical issues and constraints.

Throughput: The maximum throughput of the Bitcoin network is now 7tps (transactions per second). Two other networks for processing transactions are VISA (2,000tps) and Twitter (5,000tps). The blockchain network's throughput has to be raised if the frequency of transactions is to remain constant. Latency: Currently, a transaction must take place over a period of around 10 minutes in order to maintain the confidentiality of a Bitcoin transaction block. In a few seconds, a block can be created and the transaction confirmed. For instance, it doesn't take long to complete a transaction using VISA.

DOI: 10.17148/IJARCCE.2023.12218

Volume and bandwidth: The current size of the Bitcoin blockchain is over 50,000MB (February 2016). If throughput hits VISA levels, the blockchain might gain 214PB annually. The Bitcoin community believes that each block is IMB in size and that a new block is created every 10 minutes. Thus, there are a finite number of transactions (on average, 500 per block). The size and bandwidth issues must first be resolved if the blockchain is to support an increase in the number of transactions.

1.5.1 Security:

The way the current Blockchain is constructed makes it susceptible to a 50% attack. A single organisation would be in charge of the majority of the network's mining hash rate, giving it the ability to affect Blockchain. To fix this issue, more security research is needed.

1.5.2 Resources that been frittered:

Bitcoin mining is a daily waste of billions of dollars. The Proof-of-Work effort in cryptocurrencies is to blame for wasting Bitcoin's resources. While using Proof-of-Stake, resources are compared based on a miner's Bitcoin holdings. If someone owns 1% of bitcoin, they are allowed to mine 1% of the blocks that show their ownership. The issue of wasted resources needs to be addressed and fixed in order to increase the effectiveness of mining in Blockchain.

l. 5.3 User-friendliness:

It's difficult to use the Bitcoin API to build services. A better developer-friendly API is needed for Blockchain. REST APIs are a prime illustration of this.

Versioning, hard forks, and various chains of code are all present. Chains with fewer nodes are more likely to experience 51 percent attacks. Another issue emerges when chains are divided for administrative or versioning purposes.

l. 6 Decentralized (Autonomous) Organization:

As a result, the idea put out by Michael Jensen and William Mackling that entities are nothing more than a set of agreements and links has come to pass. Since 2013–2014, Bitcoin, the first decentralised public ledger in the world, has gained popularity. Although widespread acceptance is still a ways off, the blockchain technology that underpins Bitcoin may be responsible for its success. A shared electronic public ledger system accessible to all users via the Internet or another wide-area network of computers. With the notable exception of token-free apps, blockchain is often made to do away with the need for a reliable third party to verify transactions. The next paragraphs will go over five of the most crucial traits of public ledgers.

Even while Blockchain seems to be a viable choice for carrying out cryptocurrency transactions, it still has several technical issues and limitations that need to be researched and resolved in the future. Blockchain transactions must have high integrity and security, as well as node privacy, to prevent attacks and attempts to disrupt them. In addition, a lot of computational power is required for the Blockchain to verify transactions.It is crucial to acknowledge and comprehend what areas have already been researched and dealt with in Blockchain as well as what the present main issues and limitations are that need more research. Finding pertinent Blockchain-related papers required a rigorous mapping study methodology. The comprehensive mapping inquiry scanned scientific databases using a well-designed approach. The map of current Blockchain research will help researchers and practitioners identify potential study topics and problems for future research.

1.7 Issues with Blockchain Technology:

Almost everyone would concur that blockchain technology has the potential to significantly change banking and economics in the near future, among other aspects of society. This cutting-edge technology faces a number of obstacles on the way to becoming a significant ecosystem for the global financial network. Despite the fact that cryptocurrencies and blockchain technology have many advantages, there are many factors that prevent them from becoming a universal standard for financial transactions. Users are worried when there are no rules.Having legal standing as a way to create a long-term payment scheme the goal of standardising market elements and lowering volatility is to Another major worry associated with the lack of rules is the use of cryptocurrencies in financial crimes and money laundering, as well as their use by the black market. Because of the design of the blockchain network, users may also experience the highest level of anonymity. Using cryptocurrencies to access blockchains and commit crimes now allows criminals and drug dealers to hide their identities, but it has also given them new opportunities. To stop such crimes from happening in the first place, significant legal reforms are required.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12218

Although blockchain is a well-liked alternative to traditional systems for record-keeping and money transfers due to its innovative technology, it is still vulnerable to hacker attacks. Blockchain technology was not employed in any recent cryptocurrency-related hacking incidents; instead, digital currency exchanges were targeted. Network security for cryptocurrencies has never been breached by hackers. The security protocol used at digital currency exchanges must be implemented and maintained by each exchange. However, the perceptions of current and potential consumers are negatively impacted by these hacking stories. Without a doubt, news of hacking occurrences at exchanges has contributed to a negative perception of cryptocurrencies and blockchain that has yet to be dispelled.

1.8 Critics of public ledgers: Moving toward hybrid solutions?

Technology has always offered a mechanism to transfer power from a centralised government to the people. Early mechanical developments made it possible for people to keep track of their own time several centuries ago, just as large, expensive clock towers served as symbols of the consolidation of power in the hands of a select few. The blockchain is in conflict with the fundamental ideas of traditional banking.

The tendency of an accountant is to compile all payment, transaction, and loan data into a computer system.The main responsibility of a banker is to safeguard both money and financial data. Blockchain technology has the potential to revolutionise the financial industry as a whole. examining potential uses that could boost financial institutions' productivity and cut expenses.

We examine the benefits and drawbacks of this newly developed decentralised technology and make the case that widespread adoption will result in the expansion of a new branch of law known as Lex Cryptographia, which consists of regulations that are enforced by decentralised (autonomous) organisations and self-executing smart contracts. Due to the widespread adoption of blockchain technology, governments and huge multinational organisations may no longer be able to regulate and affect the behaviour of many people in traditional ways.

This suggests that it will become more crucial to have a thorough understanding of how to manage blockchain technology and how to oversee the development and deployment of these new decentralised organisations in ways that are not currently covered by existing legal theory.

II. DISCUSSION

Cryptocurrencies like Bitcoin and Ethereum have the power to significantly alter our societies. The hazards and benefits of its potential usage must, however, be carefully weighed in order to avoid utopian goals and the pitfalls of technocratic thinking and predestination. It is practicable and desirable to permit the decentralisation of government services via a permissioned blockchain since it can increase the effectiveness of those services. The risks and drawbacks of decentralising governance through open, distributed blockchains, like Bitcoin, however, outweigh the advantages. Fully distributed blockchain ecosystems are characterised by significant knowledge and power asymmetries between developers and customers, in addition to a high number of third parties and successful businesses providing intermediary services.

Due to the concentration of power in the hands of a few numbers of influential technologists and the lack of transparency in decision-making, the egalitarian nature of existing dispersed networks is called into question, which makes the hopes of some blockchain proponents unachievable. In reality, authority is more nuanced, therefore the idea of a blockchain-based authority is deceptive. There are so reasons to doubt the blockchain-based governance's ability to effectively facilitate individual power in a general sense. The promise of empowering individuals is probably going to fall short due to the importance of markets and the speculative verification techniques used by fully distributed blockchains. The practise of depreciating public institutions, prioritising economics over politics, and turning citizens into customers with the promise of greater freedom and efficiency as well as better equality may be covering up yet another evil development. In reality, there have been significant social and financial consequences associated with this type of power shift for decades and in a variety of ways.

The very democratic foundations that libertarians today seek to defend are susceptible to being undermined by antipolitical forces. Even worse, these agents may consciously pursue a divide and imperia strategy between civil society and the state in order to undermine the traditional democratic order, alter existing power balances, and establish dominance in society. This would be a business model that would make overthrowing the State and absorbing its functions profitable. In any case, a few friends might amass sufficient wealth to establish a totalitarian government. If the neo-liberal ascendancy and its corporate objective establish their own brand of democracy, a decentralised algorithm-based society is a feasible premise.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12218

III. CONCLUSION

The majority of techno-libertarians think that since unified vertical authority is destructive to individual powers, the ability of the block chain to generate consensus across participants on a large scale is especially crucial. They frequently promote a utopian image of a non-hierarchical, non-coercive society governed by algorithm-based consensus, where people can communicate freely. Other ICT cliches have emerged during the past few decades, including "the notion of a better government" and "the idea of an attentive and empowered client." We will quickly go over the reasons why hierarchical enterprises in society or the political problem of coercion cannot be solved by blockchain governance. It follows logically that blockchain-based governance should be seen as an institutional theory with utmost technical and management interest for market, private services and section, rather than a political view in and of itself. The use of leading edge and blockchain technology as pre-political tools can be distinguished similarly. Otherwise, when it comes to how internationalisation operates and the free market, blockchain-based governance can be regarded as immoral anti-politics glammed up in language of inevitability. The challenge will be to combine disruptive technology like blockchain with citizen rights, equality, social cohesion, inclusion, and public sector protection as global civil society explores new political and social dimensions. To more accurately assess the risks, merits, and consequences of emerging technology, all fields of human knowledge must collaborate in mature, multidisciplinary research projects, paying particular emphasis to political theory, the humanities, and social sciences.

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. I 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 10T 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-08-2018099.
[9] L. C. Arcos, "The blockchain technology on the music industry," Brazilian J. Oper. Prod. Manag., 2018, doi:10.14488/bjopm.2018.vl 5.n3 .al l.
[10] A Tilooby, "The Impact of Blockchain Technology on Financial Transactions," August 14, 2018.