Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 22 Issue 1, January 2020

Block chain and Its Current Applications: A Critical Analysis

Dr. Mamta Bansal, Mr. Anuj Kumar
Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- mamta.bansal@shobhituniversity.ac.in, anuj.k@shobhituniversity.ac.in

ABSTRACT: Blockchain has the potential to address these key issues. Bitcoin, along with blockchain, was created as the first and most widely used cryptocurrency. Since the advent of Bitcoin, the first and biggest cryptocurrency, block chain technology has been recognized as a digital currency platform. It has previously been used for decentralization of markets in general, rather than just decentralization of money and payments. The block chain's decentralized transaction ledger may be used to register, confirm, and transmit various types of contracts to other network participants. We fully examine state-of-the-art block chain-related applications that have appeared in the literature in this article. A number of previously published publications were carefully considered for inclusion based on their contributions to the block chain body of knowledge. In the last part of the article, many points are examined and debated.

KEYWORDS: Blockchain, Biot, Cryptocurrency, Distributed Systems, Traceability.

INTRODUCTION

The digital, distributed, and decentralized ledger that represents the majority of virtual currencies and is responsible for recording all transactions without the need for a financial intermediary such as a bank. To put it another way, it's a new way of sending money and storing data. Blockchain is the brainchild of engineers who saw flaws in the existing financial system[1]. They laughed at the notion that payment validation and settlement might take up to five business days in cross-border transactions, since they saw banks acting as third parties and collecting transaction fees needlessly. Real-time transactions (even across borders) are possible with blockchain, and banks are removed from the equation completely, potentially lowering transaction costs. Blockchain may be used for a variety of purposes other than money. Several Dow Jones Industrial Average components are now putting some of these applications to the test in small-scale initiatives and controlled demonstrations. A software system may be classified into one of two architectural approaches: centralized or distributed. The nodes of a centralized software system are dispersed across the system linked to a single central coordinating node Distributed On the other hand, a system with many linked nodes without any central control node The difference is striking. a combination of these two designs There are many advantages to having a Having greater computational power by using a distributed system Using the combined processing capacity of all linked nodes, because it doesn't have a battery, it has a higher level of dependability a single instance of failure, and so forth. However, there are a few disadvantages. Communication overhead and the cost of maintaining a distributed system are two factors to consider[2]. security concerns relating to unauthorized access to a network node that are untrustworthy in the meanwhile, blockchain may be considered a component of the implementation. a distributed software system's layer The Information It is possible to establish and preserve integrity in distributed systems. using the

blockchain Furthermore, blockchain has the potential to. It may also be seen as a purely peer-to-peer system. made composed of a network's individual nodes Dishonest and malevolent peers constitute the most serious danger to the integrity of the system peer-to-peer networks Individual nodes attempt to take advantage of the situation. system for their own goals, since there are no recognized peers with whom they may compare notes[3]. There may be an undetermined level of dependability and trustworthiness. Thus, Blockchain has the potential to address these key issues. Bitcoin, along with blockchain, was created as the first and most widely used cryptocurrency. When a centralized system is used, it allows for trustless and reliable transactions. Despite the consumers' lack of confidence, administration is not needed. Users in the network are either untrustworthy of each other or there are untrustworthy users in the network. Since then, blockchain has attracted a lot of interest feature for a decentralized transaction ledger that may be used to register, confirm, and transmit contracts and payments. In addition, blockchain technology has been used in a variety of ways. financial transactions, as well as any other kind of transaction or application healthcare, utilities, real estate, and government, to name a few.5th sector as a result of the blockchain, these are proven to be viable[4]. Bitcoin's structure is both portable and extendable. Initially, the primary use of blockchain was to link coins. with traditional financial and banking institutions Due to its advantages over conventional currencies, the usage of cryptocurrencies based on blockchain technology is expected to revolutionize payments. Due to the elimination of intermediaries, merchant payment costs may be lowered to less than 1%, and consumers can get money instantly rather than waiting days. Cryptocurrencies nowadays may be broken down into three categories. The terms blockchain, protocol, and money are all used interchangeably. It should be noted that although a coin may have its own currency and protocol, its blockchain may be based on another coin's blockchain, such as Bitcoin or Ethereal. Counterparty, for example, has its own money and system, although it is based on the Bitcoin network[5].

The blockchain serves as a ledger in the case of cryptocurrencies, storing all of the coin transactions that have occurred. This implies that the blockchain is always growing, with new blocks being added at regular intervals. A complete node (a machine that verifies transactions) holds a copy of the whole blockchain, which includes data on user addresses and balances. If the blockchain is open to the public, it may be searched using a block explorer such as Blockchain.info to retrieve the transactions associated with a certain address[6]. As a result, the most important value of blockchain is that it allows you to conduct transactions with another person or organization without relying on third parties. This is a viable option. owing to a large number of decentralized miners (accountants) that examine and verify each transaction This contribution enabled the Bitcoin blockchain to solve the Byzantine Generals' Problem, as it allows multiple parties (generals) who do not trust each other to agree on something (a battle plan) by only exchanging messages, which could come from malicious third parties (traitors) attempting to deceive them[7]. This computational problem is related to the double-spend problem in the case of cryptocurrencies, which deals with how to confirm that some amount of digital cash has not already been spent without the validation of a trusted third-party (typically, a bank) that keeps track of all transactions and user balances. Because there are numerous entities (nodes, gateways, and users) in an IoT system that do not necessarily trust one other while conducting transactions, IoT has certain similar issues with cryptocurrencies. However, there are many factors that

distinguish IoT from digital currencies, such as the amount of processing power available in nodes or the need to reduce energy consumption in battery-powered devices[8].

As a result, despite its present practical limitations, this study investigates such parallels and examines the benefits that blockchain may offer to IoT. Furthermore, the major Blockchain-based IoT (B IoT) designs and suggested enhancements are examined. The most important future difficulties for the use of blockchain to IoT are also discussed. Other writers have already provided surveys on block chain's applicability in other areas. For example, it contains a thorough explanation of the fundamentals of blockchain and smart contracts, as well as a good overview of the application and deployment of B IoT solutions. However, while the paper contains a wealth of information, it does not go into detail about the characteristics of an ideal B IoT architecture or the possible optimizations that can be made when developing B IoT applications. Another intriguing paper is, in which the authors give a broad overview of the architecture and various processes involved in blockchain, but it is not specifically focused on its application to IoT. Similarly, different researchers provide overviews of blockchain in and, but they emphasize its application to various Big Data areas and a variety of industrial applications. Finally, the systematic reviews provided are worth noting since they examine the types of issues that publications in the literature deal with when suggesting the usage of blockchain. Unlike the previous evaluations, this study takes a comprehensive approach to blockchain for IoT scenarios, covering not only the fundamentals of blockchain-based IoT applications, but also a detailed examination of the most important elements of their creation, deployment, and optimization[9].

This study also aims to envisage block chain's potential contribution to modernizing the IoT sector and addressing current problems. The rest of this paper is laid out as follows. The second section covers the fundamentals of blockchain technology. How they operate, what kinds are available, and how to determine whether or not a blockchain is suitable to employ. The most important B IoT applications are presented in Section III. Section IV examines key elements of a blockchain that must be improved in order to adapt it to an IoT application. Section V highlights the major flaws in today's B IoT applications as well as the major technological difficulties they confront. Section VI highlights further medium-term issues and offers advice to IoT developers. The last section, Section VII, is dedicated to the conclusion. A blockchain is a distributed ledger that allows data to be shared among a group of people. As previously stated, it is regarded as Bitcoin's most important contribution since it addressed a long-standing financial issue known as the double-spend problem. The solution suggested by Bitcoin was to seek the consensus of the majority of mining nodes, which would then add legitimate transactions to the blockchain. Although blockchain was created as a platform for cryptocurrency development, it is not need to generate a cryptocurrency in order to utilize it and construct decentralized apps.

A blockchain is a series of timestamped blocks connected by cryptographic hashes, as the name suggests. The next subsections explain the fundamental features and functionality of a blockchain to familiarize the reader with its inner workings. To utilize a blockchain, you must first set up a peer-to-peer network with all of the nodes that want to use it. Every node in the network is given two keys: a public key that other users use to encrypt messages sent to it, and a private key that enables the node to read those messages. As a result, two keys are utilized, one for encryption and the other for decryption. In reality, the private key is used to sign blockchain transactions (that is,

to authorize them), while the public key acts as a unique address. The communications encrypted with the associated public key can only be decrypted by the person who has the appropriate private key. Asymmetric cryptography is the term for this. The scope of this article does not allow for a comprehensive description of its inner workings, but interested readers may find more information[10].

After completing a transaction, a node signs it and broadcasts it to its one-hop peers. The fact that the transaction is signed in a unique manner (using the private key) allows it to be authenticated (only the user with a particular private key may sign it) and ensures integrity (the data will not be decrypted if there is a mistake during transmission). When the peers of the node that broadcasts the transaction get the signed transaction, they check that it is legitimate before retransmitting it to additional peers, helping the transaction spread across the network. Special nodes called miners order and pack the transactions disseminated in this way that are considered valid by the network into a timestamped block, with the data included in the block being determined by a consensus algorithm a more detailed definition of the concept of consensus algorithm is given later in Section IV-D. The miner's blocks are subsequently broadcast back into the network. The blockchain nodes then check that the broadcast block includes legitimate transactions and that it uses the corresponding hash to refer to the previous block on the chain. The block is discarded if these criteria are not met. However, if all criteria are met, the nodes add the block to their chain and the transactions are updated. There are many kinds of blockchains based on the data that is maintained, the availability of that data, and the activities that may be done by a user. As a result, public and private blockchains, as well as permissioned and permission less blockchains, may be differentiated.

DISCUSSION

It's worth noting that some authors use the terms public permission less and private/permissioned interchangeably, which is fine when discussing cryptocurrencies but not when discussing IoT applications, where it's critical to distinguish between authentication who can access the blockchain; private versus public) and authorization what an IoT device can do; However, keep in mind that such differences are still up for dispute, and the definitions presented here may vary from those found elsewhere in the literature. Anyone may join a public blockchain without the permission of a third party, and they can serve as a basic node or a miner/validator. In public blockchains like Bitcoin, miners and validators are typically compensated financially. In the case of private blockchains, the owner controls who has access to the network. Many private blockchains are permissioned to control which users can perform transactions, execute smart contracts (a concept defined later in Section III), or act as miners in the network, but this is not true of all private blockchains. For example, a company may create a permission less private blockchain based on Ethereal. Hyper ledger Fabric and Ripple are two examples of permissioned blockchains. It's also important to distinguish between blockchains that are solely for tracking digital assets (e.g., Bitcoin) and blockchains that allow for the execution of logic (e.g., smart contracts). Furthermore, some systems (like as Ripple) utilize tokens, while others do not (e.g., Hyper ledger). It's worth noting that such tokens aren't always linked to the existence of a cryptocurrency, but they may be used as internal receipts to show that particular actions occurred at certain times. Before getting into the specifics of how to utilize a blockchain for IoT applications,

it's important to note that a blockchain isn't the ideal answer for every IoT situation. Traditional databases or ledgers based on Directed Acyclic Graph (DAG) may be a better match for certain IoT applications. To evaluate if the usage of a blockchain is suitable, a developer should consider whether the following characteristics are required for an IoT application. Decentralization. When there isn't a trustworthy centralized system, IoT applications need decentralization. Many people, however, continue to blindly trust specific businesses, government organizations, or banks, thus a blockchain is not needed if mutual trust exists. P2P (peer-to-peer) exchanges.

The majority of IoT connections are routed via gateways to a distant server or cloud. Except for specialized applications, such as intelligent swarming or mist computing systems peer-to-peer communications at the node level are uncommon. Other models, such as fog computing with local gateways, encourage communication among nodes at the same level. System of payment Some IoT applications may need doing financial transactions with other parties, while many do not. Furthermore, conventional payment methods may still be used to conduct economic transactions, but they typically require the payment of transaction fees and the confidence of banks or intermediaries. Distributed system with a lot of sturdiness. Clouds, server farms, and other conventional distributed computing systems may all be used to create distributed systems. The need for this feature alone is insufficient to justify the deployment of a blockchain: there must also be a lack of confidence in the person in charge of the distributed computing system. Blockchain technology may be used in a variety of areas and scenarios. According to some writers, the development of blockchain applicability began with Bitcoin (blockchain 1.0), then progressed to smart contracts (blockchain 2.0), and finally to justice, efficiency, and coordination applications. Smart contracts are described as bits of self-contained decentralized code that run autonomously when specific criteria are fulfilled. Smart contracts may be used in a variety of situations, such as foreign payments, mortgages, and crowd financing. Although Ethereum can run other distributed apps and connect with other blockchains, it is probably the most popular blockchain-based platform for executing smart contracts.

In reality, Ethereum is Turing-complete, a mathematical notion that means Ethereum's programming language can mimic any other language. The scope of this article does not allow for a comprehensive explanation of how smart contracts operate, but the interested reader may find a very excellent description in Section II. The letter D. IoT agriculture applications may also benefit from blockchain. A traceability system for monitoring Chinese agro-food supply, for example, is described in. The system is built on the usage of Radio Frequency Identification (RFID) and a blockchain, with the goal of improving food safety and quality while reducing logistical losses. Other academics worked on using a blockchain to manage IoT devices. Researchers developed a method that could remotely operate and configure IoT devices. Private keys are kept on each IoT device, while public keys are stored on Ethereum. The authors claim that using Ethereum is critical since it enables them to build custom code that runs on top of the network. Furthermore, changing the code on Ethereum changes the behavior of IoT devices, making maintenance and bug fixes easier.

The use of a blockchain to IoT or the Internet of Energy (IoE) may also help the energy industry gives an example of a blockchain-based system that enables IoT/IoE devices to pay each other for services without the need for human involvement. The article describes an implementation that

demonstrates the system's potential: a smart cable connected to a smart socket may pay for the energy used. In addition, the researchers propose a single-fee micro-payment protocol that combines many small payments into a bigger transaction to decrease transaction costs for cryptocurrencies like Bitcoin. Healthcare B IoT applications have also been documented in the literature. In for example, a traceability application is described that uses IoT sensors and blockchain technology to ensure data integrity and public access to temperature records in the pharmaceutical supply chain. This verification is essential for medical product transportation in order to guarantee product quality and environmental conditions (i.e., their temperature and relative humidity).

As a result, every delivered package has a sensor that collects data and sends it to the blockchain, where a smart contract decides if the received values are within the permitted range. The design of a blockchain-based platform for clinical trials and precision medicine, which is another healthcare B IoT application. It's also worth noting, which describes a general smart healthcare system that incorporates IoT devices, cloud and fog computing, a blockchain, and message brokers. Blockchain technology may help improve IoT low-level security. It may be enhanced in particular for remote attestation, which is the process of determining if a device's underlying Trusted Computer Base (TCB) is trustworthy. This may be done by controlling the TCB measurements acquired using ARM Trust Zone and a blockchain, where they are securely kept. Smart cities and industrial processes are two more B IoT applications that have previously been suggested. In the instance of a framework is provided for delivering smart city apps that combines smart devices in a safe manner. Different blockchain-based industrial applications, as well as their connections to Industrial IoT networks, are discussed in. Finally, since blockchain technology may be used to utilize Big Data (i.e., to guarantee its trustworthiness), some academics evaluated the major blockchain-based systems for gathering and controlling large quantities of data gathered via IoT networks. Three architectures may be seen to rely on a cloud, but the degree of reliance varies greatly in reality. In a cloud-based architecture, data gathered by the Node Layer is sent directly to the cloud through IoT gateways, requiring no further processing beyond that required for protocol conversion (in case it is needed).

There are more complex gateways, but in most cloud-based applications, the majority of processing is done in the cloud. However, conventional cloud-based IoT designs have certain inherent weaknesses, the most important of which is the fact that the cloud is a single point of failure: if the cloud goes down due to cyberattacks, maintenance, or software issues, the whole system stops functioning. Furthermore, it is critical to highlight that if a single IoT device is hacked, it has the potential to disrupt the whole network by launching DoS attacks, eavesdropping on private data [81], changing the acquired data, or deceiving other systems. As a result, if one IoT device linked to the cloud or a central server is hacked, the rest of the nodes may be vulnerable. Blockchain-based solutions, on the other hand, do not depend on a single central server or cloud. Furthermore, since transactions are cryptographically validated, the system may reject blockchain updates if harmful activity from a hacked device are discovered.

The other two are newer and offload some of the computation from the cloud to the network's edge. This offloading is critical for IoT applications because, if the number of IoT connected devices continues to grow at the current pace the quantity of communications that must be handled

by a cloud will skyrocket, necessitating the expansion of cloud network capacity. Edge and fog computing may therefore be utilized to enable geographically dispersed, low-latency, and applications, reducing network traffic and processing burden in conventional cloud computing systems. Fog computing is built on a network of local gateways that can react quickly to requests from IoT nodes through specialized services. These nodes may also communicate with one another and, if necessary, with the cloud for instance, for long term storage. The primary benefit of cloudlets is that they can offer high-speed answers to compute-intensive activities needed by the Node Layer (for example, operating a complete node of a blockchain), which are unable to provide efficiently using resource-constrained fog gateways. Other designs have been investigated in the past to address the architectural challenges that emerge while delivering B IoT services. A succinct but useful list of options. The benefits and drawbacks of four alternative architectures (dubbed Fully Centralized, Pseudo-Distributed Things, Distributed Things, and Fully Distributed by the authors) are explored in such a study. The researchers believe that a B IoT design should be as similar to the Fully Distributed method as feasible, but that alternative techniques may be more suitable in certain situations when computing power or cost are limiting considerations.

IBM's ADEPT is an intriguing platform that encourages decentralization for IoT devices. A platform like this was created for safe, scalable, and self-contained peer-to-peer IoT telemetry. ADEPT is provided more as a starting point for debate than as an implementation, according to the authors, although its white paper offers a comprehensive explanation of the platform's needs. The researchers point out that an IoT device should be able to authenticate and maintain itself, leaving the burden of registering new devices in the blockchain to the makers. Furthermore, ADEPT's concept of mining differs from the one used in Bitcoin.

CONCLUSION

The pace of technical advancement in an Internet-enabled global society, the growth of social problems, and growing competition for limited resources are all speeding up the transition to a data-driven world. In this environment, blockchain can provide a platform for IoT to distribute trustworthy data that is independent of non-collaborative organizational hierarchies. This study looked at the current status of blockchain technology and suggested major possibilities for IoT applications in areas including healthcare, logistics, smart cities, and energy management. These BIoT situations have unique technological needs that vary from cryptocurrency implementations in many ways, such as energy efficiency in resource-constrained devices or the necessity for a particular design. The goal of this study was to assess the practical constraints and suggest potential research topics. Furthermore, it provided a comprehensive approach to BIoT scenarios, including a detailed examination of the most important elements of an optimal BIoT design, such as its architecture, necessary cryptographic algorithms, and consensus mechanisms. Furthermore, certain suggestions were made with the goal of guiding future BIoT researchers and developers through some of the problems that will need to be addressed before the next generation of BIoT applications can be deployed.

REFERENCES

[1] P. Middleton, P. Kjeldsen, J. Tully, and K. Findings, “Forecast: The Internet of Things, Worldwide,” 2013.

[2] P. Middleton, T. Koslowski, and A. Gupta, “Forecast analysis: Internet of Things--endpoints, worldwide, 2016 update,”

Gart. Database (ID G00302435).(February 2017), 2017.

[3] M. Shirer and E. Smith, "IDC Forecasts Worldwide Spending on the Internet of Things to Reach $772 Billion in 2018," *IDC press*. 2017.

[4] D. Drescher, *Blockchain basics: A non-technical introduction in 25 steps*. 2017.

[5] A. Judmayer, N. Stifter, P. Schindler, and E. Weippl, "Blockchain: Basics," in *Business Transformation through Blockchain: Volume II*, 2018.

[6] S. Brakeville and B. Perepa, "Blockchain basics: Introduction to distributed ledgers," *IBM developerWorks*. 2017.

[7] T. Hoser, "Blockchain basics, commercial impacts and governance challenges.," *Gov. Dir.*, 2016.

[8] D. Appelbaum and S. Stein Smith, "Blockchain Basics and Hands-on Guidance - The CPA Journal," *CPA J.*, 2018.

[9] Y. A. Pignolet and T. Locher, "Blockchain - Basics and beyond," *ABB Rev.*, 2018.

[10] D. Drescher, *Blockchain Basics*. 2017.