Survey on Blockchain - Applications, Features and Challenges

M Nagarani, Research Scholar, Department of Computer Science, Dr. N.G.P Arts and Science College, Coimbatore, India, nagaraniresearch@gmail.com

A Nirmala, Research Supervisor, Department of Computer Science, Dr. N. G.P Arts and Science College, Coimbatore, India , nirmala@drngpasc.ac.in

Abstract - Blockchain is a promising technology due to its features of consensus-driven Distributed ledgers maintained by distributed network computing systems. This has created an exciting possibility of data performance, Immutability, and authenticity enabling transactions in a trustless business scenario and new business model. In particular, when compared to other modern technologies like Big Data, Cloud Computing, and the Internet of Things, the blockchain offers a security framework to safeguard the object's privacy. One of the most promising new technologies to emerge in the last ten years is blockchain. The majority of the next research projects are being developed to fully understand blockchain technology. In this paper, researchers can explore various Features, Challenges and Applications in Blockchain Technology.

Keywords* — *Blockchain, Applications, Features, Challenges, Internet of Things, Smart Contract, Decentralization

I. Introduction

Blockchain began in 1991 as a method of storing and securing digital data. With the help of innovative database technology called blockchain, a corporate network can transparently share information. A blockchain database stores information in blocks linked in a chain. Blockchain is the foundation of a decentralized society. Our existing ecology is entirely centralized, which means that only a small number of people have the authority to make choices [1]. Whereas a decentralized is with any authority, the power is distributed among all the members of the network [2]. Weichao Gao, William G. Hatcher, and Wei Yu described that the unceasing growth of the Internet of Things (IoT), Cloud and Edge Computing, and Big Data are rapidly necessitating novel solutions to manage distributed and decentralized systems. Additionally, in the era of those areas, the enforcement of secure, trusted, and verifiable services is paramount, as the volume of network-connected user data and vulnerable devices is unprecedented and increasing. Sadly, trust is in increasingly short supply, as the frequency of data breaches at monolithic software companies continues apace, exposing massive amounts of private information. The blockchain is a shared public ledger that records all confirmed transactions. It consists of blocks that hold batches of valid transactions. Blockchain is a type of data structure that allows for the establishment of a peer-to-peer distributed ledger that cannot be altered.

II. LITERATURE SURVEY

Weichao Gao, et al., in the paper entitled "A Survey of Blockchain: Techniques, Applications, and Challenges", state that, To decentralize services, security, and verifiability, blockchain provides a peer-to-peer network in which distributed nodes work together to confirm transaction provenance. Users and service providers are placed in an asymmetrical relationship due to centralization, which presents a single point of failure for attackers to exploit. Centralization is a major weakness of numerous software designs. Pinyaphat Tasatanattakool, et al., in the paper entitled "Blockchain: Challenges and Applications", summarizes that the Blockchain is a database that is used to store information in a decentralized network. Blockchain, on the other hand, is not limited to financial applications. Qalab E Abbas, et al., "A Survey of Blockchain and Its Applications", this paper reviews the structure of the Blockchain and discovers various applications of the blockchain. Akanksha Kaushik, et al., “Blockchain – Literature Survey”, this paper describes Online and digital transactions using Bitcoin and the comparison of Centralization and Decentralized concept of Blockchain technology. Junfeng Xie, et al., in the paper entitled “A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges”, states that the brief information about the blockchain and blockchain-enabled smart cities. Kanika Agrawal, et al., in the paper entitled “An Extensive Blockchain Based Applications Survey: Tools, Frameworks, Opportunities, Challenges and Solutions”, proposed literature on the various applications,

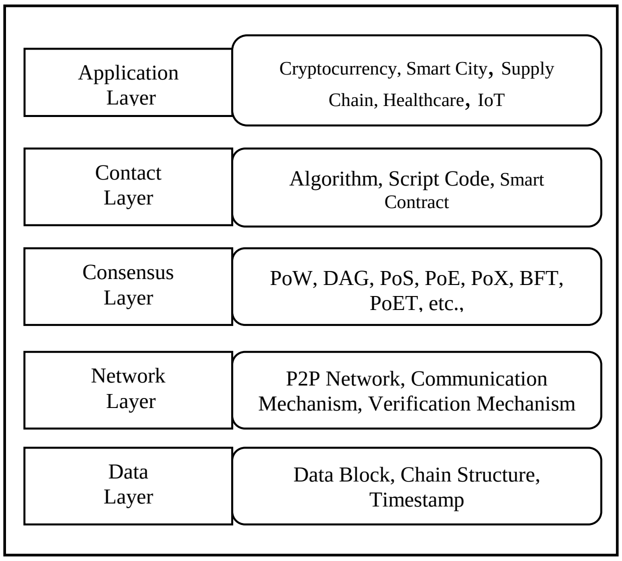
DOI : 10.35291/2454-9150.2024.0006

including those in agriculture, aviation, banking systems, and other areas, there are several security standards and cryptographic solutions available. However, merging existing technologies with blockchain can result in a more effective and efficient solution The shortcomings of earlier research, including scalability, immutability, resilience, network latency, auditability, and traceability, are addressed in this study. This study gives a comprehensive review of ten various blockchain applications and tools to synthesize the prior research. This research provided a taxonomy for these applications and examined how tools were implemented across various disciplines. Additionally, other outstanding problems, difficulties, and critical blockchain technology lessons were emphasized. Ahmed Afif Monra, et al., in the paper "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities," precise the open challenges, characteristics of the Blockchain technology, and the transaction process of the Bitcoin transactions and Ethereum transactions.

With the aid of the earlier existing solutions proposed by various researchers, our survey provides a detailed study of blockchain technologies and their challenges that help the researchers explore further in a proper direction.

III. BLOCKCHAIN: AN OVERVIEW

Blockchain is a Distributed ledger governed by a peer-to-peer network. In a simple manner distributed database, which is accessible and visible to all stakeholders involved to have a trusted and transparent data sharing and information symmetry. Blockchain is a multidisciplinary field, which deals with concepts of verifiable services that are paramount, as the volume of network-connected user data and vulnerable devices is unprecedented and increasing. Sadly, trust is in increasingly short supply, as the frequency of data breaches at monolithic software companies continues apace, exposing massive amounts of private information [3].



Application Laver	Cryptocurrency, Smart City, Supply Chain, Healthcare, IoT
Contact Layer	Algorithm, Script Code, Smart Contract
Consensus Layer	PoW, DAG, PoS, PoE, PoX, BFT, PoET, etc.,
Network Layer	P2P Network, Communication Mechanism, Verification Mechanism
Data Layer	Data Block, Chain Structure, Timestamp

Figure 1 Blockchain Framework in Layers

The blockchain is a shared public ledger that records all confirmed transactions. It consists of blocks that hold batches of valid transactions [4]. Blockchain is a data structure that enables the creation of a tamper-proof distributed ledger in a peer-to-peer setting [5].

In a nutshell, a chain of connected blocks (also known as Nodes) can be used to conceptualize blockchain. For every new transaction or update, a consensus must be reached for verification. The nodes of the network can agree on various methods for this verification process. Due to its distributed ledger technology, Blockchain eliminates the risk of potential fraud by prohibiting any modifications once consensus is reached, thus guaranteeing that the data stored in Blockchain networks are secured and reliable.

Blockchain can be thought of, in a limited view, as a chain of linked data blocks, each dependent on the prior block, forming a continuous, chain-like data structure. Blockchain is composed of essential and supporting components, including the interaction environment and applications, which form an integral part of the overarching framework. Figure 1 illustrates the layered structure of Blockchain technology. Blockchain technology can be split into distinct components which are Application Layer, Contact Layer, Consensus Layer, Network Layer, and Data Link Layer. These layers work together to enable more secure transactions and to make it easier for businesses to operate using this technology.

IV. UNITS

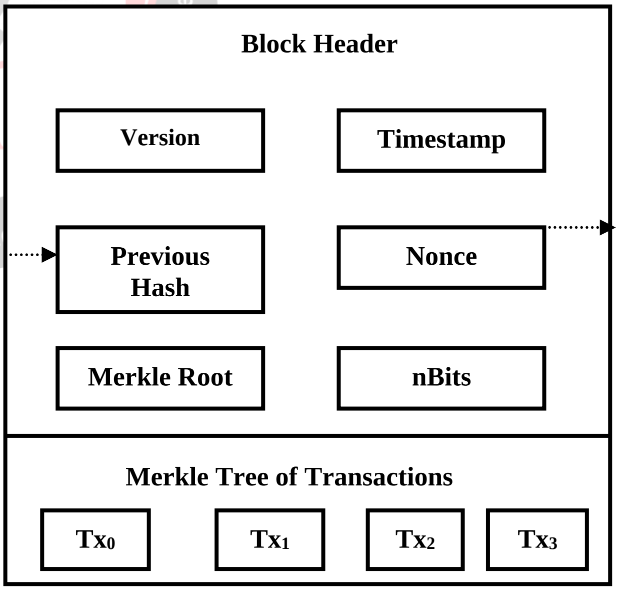


Figure 2 Block Structure in Blockchain

Figure 2 illustrates the structure of the blocks. Block structure mainly includes two parts: the block header and the block body. The Block body consists Merkle tree of transactions. The table represents the sub-parts of the Block Structure. The metadata is listed in the block header and includes the timestamp, Nonce, and Merkle root, the hash of the current block, the hash of the preceding block, and

DOI : 10.35291/2454-9150.2024.0006

the [6] version. The technical terms for data blocks in blockchain, which include version, previous hash, timestamp, nonce, Merkle root, and nBits, are displayed in Table 1. A blockchain's chain is formed by the previous block hash, which connects the current block to its predecessor. The block version specifies the validation rules that must be adhered to [7]. A data structure for effectively summarizing every transaction in the block is called the Merkle root. Every block in the blockchain is uniquely identified by a hash that is produced on the block header using the SHA256 cryptographic hash algorithm. Through the "previous block hash" field in the block header, each block also makes reference to a prior block, also referred to as the parent block. In a blockchain, a timestamp is a small piece of data that is uniquely serialized and stored in each block. This information determines when block mining started and when the Blockchain network validated it. A nonce is a unique hash value that meets a predefined level of difficulty by adding a special, randomly generated number to a blockchain block. The target threshold as it appears in the block header is encoded in nBits.

TABLE 1: TECHNICAL TERMS OF DATA BLOCKS

Term	Description
Version	The version specifies the current version of the block structure
Previous Hash	The current block connects to its predecessor, known as the parent block, using the hash of the prior block.
Timestamp	The block's time of creation is indicated by its timestamp.
Nonce	A Number used once. Nonce relates to the mining process
Merkle Root	The Merkle root is the root of a Merkle tree.
nBits	nBits refers to the target. The current difficulty that was used to create this block.

IV. APPLICATIONS OF BLOCKCHAIN

Since Blockchain first became popular, extensive research has been conducted to determine what else this incredible technology might be used for. Blockchain uses are still being found, and a few of them will be addressed below.

A. Financial Application of Blockchain

A. Cryptocurrency-Bitcoin

The primary and most important application of Blockchain is in finance. It all began with Bitcoin when blockchain was used to keep a record of financial transactions, thereby eliminating the middleman. Since Bitcoin, numerous cryptocurrencies have been created using various Blockchain technologies, and hundreds of cryptocurrencies are currently traded worldwide. In Bitcoin, blocks are linked with the previous header's hash value. Every time a new transaction is made, the network gets notified of it.

These transactions are tracked by miners, who then verify them before the transaction is cryptographically secured and turned into a block. Examples of active Bitcoins are Bitbond, BitnPlay, BTC Jam, Codius, and DeBuNe [8]. Bitcoin has two major constraints that are Transactions and Miners. P2P communication, digital identity creation tools (private and public keys), and methods for users to sign documents with their private keys must exist before the Bitcoin network can begin delivering information to its peers.

Miners are core components of the Bitcoin network system. Validation of a transaction is done by miners. Also, they are responsible for mining node transactions, competing in the mining process, validating transactions, and creating new blocks. Figure 3 illustrates the blockchain in Bitcoin.

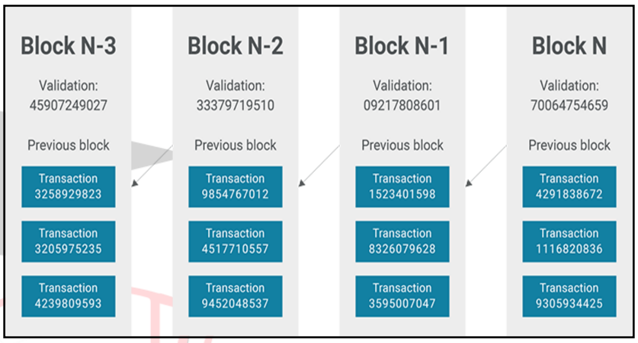


Figure 3 Blockchain- Bitcoin

B. Ripple

Ripple is a decentralized exchange with a focus on the banking market that employs ripple protocol through a peer-to-peer network for currency exchange, repatriation, and real-time gross settlement (RTGS). Coinbase, BitPesa, Billion, Stellar, Kraken, and CryptoSigma are more well-known platforms for currency exchange and transfer[8].

B. Non-financial Applications

- Ethereum

It makes use of a Blockchain-based distributed computing infrastructure and a Turing complete scripting language to facilitate the processing of smart contracts on the Blockchain [9].

C. Hyperledger

Hyperledger is a project of the Linux Foundation that creates Blockchain technologies for commercial use, and it only supports registered members. To progress Blockchain technologies among industries, Hyperledger is an open-source collaborative project. Innovators in the areas of finance, banking, the Internet of Things, supply chains, manufacturing, and technology are participating in this international collaboration, which is being sponsored by the Linux Foundation. Numerous more non-financial uses of

DOI : 10.35291/2454-9150.2024.0006

blockchain technology exist, including voting in Elections (Follow My Vote), Smart Contracts (Otonomos, Mirror, Symbiont), and blockchain in the Internet of Things (e-Plug, Filament) [10].

C. Smart Contracts

Qalab EAbbas and Jang Sung-Bong *et al* summarized Blockchain with smart contracts can eliminate the need for lawyers and intermediaries. Smart contracts will be available to all the parties and any change in the contract must be done after reaching Conesus. Smart contracts can be helpful in business as well as private dealing.

D. Internet of Things

Today, everyone's life revolves around the Internet to the point where we occasionally fail to realize just how interconnected everything is. Every gadget, including smart watches, fridges, cameras, and phones, is linked to the internet. For communication purposes, IoT always permits the transfer and exchange of data via the internet. Having a safe and secure Internet of Things has therefore become crucial [11]. The advancement of blockchain technologies, as well as their growing popularity, have prompted many to prognosticate their potential application in IoT. This is a viable option as a distributed, decentralized mechanism for ensuring credibility. IoT and similar systems for the smart world. The volume and extent of which introduce widely dispersed sensors, actuators and smart electronic devices are only growing [12]. However, the widespread use of devices with extremely little computational power for data collection and transmission presents serious security and privacy issues. As a result, it is essential to carefully evaluate and assess blockchain as it relates to IoT from all aspects [13].

E. Supply chain

To deliver a product to market, businesses must work together in supply chains. These networks, which frequently include completely unrelated parties, depend on one another's integrity to uphold laws and deliver safe goods and services.

F. Healthcare

One of the key requirements to be met is the fostering of trust in the healthcare system. The confidentiality of the patient is impacted when third parties are involved since they frequently cause data breaches and hacking. In these situations, BC stops data manipulation and fosters confidence among medical facilities, practitioners, and patients. They contribute to the trustworthiness of the healthcare management system by providing distributed storage systems, patient data safety, tamperproof data, and accuracy. In the healthcare system, a blockchain network is utilized to store and share patient data amongst hospitals, diagnostic labs, drug companies, and doctors. Blockchain applications can precisely detect serious errors, including potentially deadly ones, in the medical industry. Many recent innovations in the healthcare sector are centered on blockchain technology. Data sources, blockchain technology, healthcare applications, and stakeholders are the four conceptual layers that make up emerging blockchain-based healthcare innovations [14],[15].

G. Academics and Education System

One of the most significant issues that institutions face is establishing confidence in the academic community and educational system. Intermediaries frequently cause data breaches and have an impact on students' privacy.By eliminating any engagement from third parties, Blockchain secures the information of the students and fosters a culture of trust.

H. Agricultural System

Previously, the agricultural system encountered numerous difficulties in its implementation. Farmers were unable to gain the trust of their customers due to inadequate facilities and a lack of understanding. Uncertainty existed surrounding the specifics of the supply chain and the creation of the product from scratch. The use of intermediaries frequently leads to higher manufacturing costs and data breaches. In such cases, Blockchain is used to secure and store supply chain data, fostering trust between producer and consumer. They assist in providing agricultural supply chain data directly to buyers while also lowering agricultural transaction costs.

I. E-Voting System

The conventional voting processes were time-consuming, inconvenient, and unreliable. These systems' inaccuracy invariably leads to their inefficiency. Therefore, Blockchain was applied to produce accurate results for an effective and efficient e-voting method. It mostly aided in the complete verification and vote counting. It forbids outside parties from getting involved, which frequently leads to data breaches, and it prohibits data manipulation. It lowers the expense of the organization while facilitating voting from any location with an internet connection. All of these qualities contribute to increasing user confidence in electronic voting systems [11].

V. FEATURES OF BLOCKCHAIN

Blockchain is a distributed and decentralized database. Some characteristics of blockchain are listed and discussed below.

A. Decentralization

Each transaction in a traditional centralized transaction system must be validated by a central trusted agency. Decentralized peer-to-peer blockchain infrastructure may provide a better solution to the problem of lift resilience,

DOI : 10.35291/2454-9150.2024.0006

availability, and failover since decentralization demands trust, which is the core problem. In contrast to centralized systems, any two peers (P2P) can perform a transaction within the blockchain network without the need for central authentication. By utilizing several consensus techniques, blockchain can in this way lessen the trust issue. Further, it can alleviate performance bottlenecks at the central server and lower server expenditures (including development and operation costs) [16].

B. Persistency

Blockchain offers the framework for measuring the veracity of information and enables both data producers and consumers to demonstrate the accuracy and integrity of their data. For instance, if a Blockchain has 10 blocks, then block number 10 has the hash of the prior succeeding blocks, and the data from the current block is utilized to construct a new block. As a result, every block in the chain that already exists is linked and connected to every other block. Even transactions have connections to earlier transactions. Now, a straightforward tweak to any transaction will drastically alter the block's hash. Anyone who wishes to edit any information must alter all the hash data from prior blocks, which is thought to be an astronomically challenging undertaking given the volume of effort involved. Consequently, the network will be able to identify any data tampering or falsification. Because of this, blockchain is almost impervious to manipulation and is regarded as an immutable distributed ledger [16].

C. Anonymity

A randomly generated address can be used to interact with the blockchain network. To prevent his identity from being revealed, a user on a Blockchain network can have many addresses. No centralized organization keeps track of or collects the private information of users because it is a decentralized system. Blockchain's trustless environment contributes to some degree of anonymity.

D. Auditability

A digital distributed ledger and a digital timestamp serve as the record and verification, respectively, of every transaction that takes place within a blockchain network. As a result, previous records can be audited and traced by gaining access to any node in the network. For instance, Bitcoin allows for the iterative tracing of all transactions, facilitating the auditability and transparency of the data state in the blockchain. However, it becomes extremely difficult to track the source of the money when it is spread across numerous accounts[17].

VI. OPEN ISSUES AND CHALLENGES IN BLOCKCHAIN

This section highlights different open challenges in various application domains. such as Academics and Education, Agriculture, Banking, E-voting, Health Care, IoT, IPR, and Supply chain systems. Figure 4 shows the Taxonomy of open issues in Blockchain applications. Security tokens, database technology, smart contracts, robustness, safety, and a shifting legal environment will all determine the future of blockchain [18].While relying on the primary technologies of consensus, shared ledger, immutability, provenance, and smart contracts, the implementation and design of the BC must ensure safety, reliability, and scalability to meet the aim. This section describes the old systems' implementation and problems, as well as potential remedies offered by Blockchain technology. Applications enabled by blockchain technology are shown in Figure 4 and include Supply Chain, IoT, Banking, Agriculture, Healthcare, E-Voting, and Academics and Education.

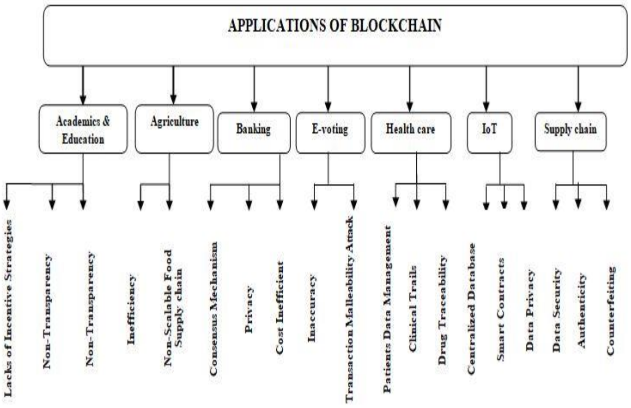


Figure 4 Blockchain applications to build trust in society: A solution taxonomy.

A. Scalability

The frequency of the blocks and their finite size to the total number of transactions that the network can support are the main issues with scalability, particularly in the traditional system. In the current environment, millions of transactions are conducted, with many of them happening in a single second. Blockchain technology aids in network scaling, hence resolving the scalability problem.

B. Privacy

The traditional system's vulnerability to information leakage is the primary cause of privacy concerns. The networks were simple targets for intrusion and attack. Therefore, BC technology uses public and private keys to assist in securing the information system in addition to privacy-preserving algorithms like SHA256 [19].

C. Centralization

The traditional system faces a significant challenge because of its centralized structure. These systems are huge and difficult for enterprises. All of the data is lost if the centralized system is attacked or corrupted. These systems also encounter network delays and demand more processing power. Usually, the system's privileges belong

DOI : 10.35291/2454-9150.2024.0006

to the central authority. As a result, it can be replaced with the BC decentralized system, which aids in data storage across all system nodes and makes the network secure against attacks and data loss [20].

D.Trust

Establishing trust was the major problem the users faced in traditional systems. Anyone trying to trust these systems found it challenging due to data leaks and attacks. Blockchain can be used to build trust in certain situations. It supports the immutable nature of the ledger and uses cryptographic methods to build Blockchain.

VII. CONCLUSION AND FUTURE WORKS

Blockchain is a ground-breaking technology that opens up new possibilities for secure, distributed applications in industries other than finance. Readers and academics might discover more about the positive aspects of blockchain technology for a range of uses by reading this study. Additionally, this survey made clear the distinctions between Bitcoin and Blockchain. The in-depth analysis of blockchain technology this paper explores the definition of Blockchain technology and its applications and integration with other technologies to support various industries in a variety of domains. As mentioned earlier, with plenty of benefits, this blockchain technology can be a perfect solution for any critical infrastructure like financial setup, healthcare, etc.

REFERENCES

[1] QalabEAbbas, Jang Sung-Bong," A Survey of Blockchain and Its Applications," in International Conference on Artificial Intelligence in Information and Communication (ICAIIC 2019).

[2] A.Kaushik, A.Choudhary, C.Ektare, D.Thomas and S. Akram, "Blockchain – Literature Survey," in 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT), India, 2017.

[3] Weichao Gao, William G. Hatcher, and Wei Yu, "A Survey of Blockchain: Techniques, Applications, and Challenges," in 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 2018. https://bitcoin.org/en/how-it-works.

[4] Scorex Foundation "A treatise on Blockchain concepts+Scorex2.0 tutorial," http://github.com/ScorexFoundation/Scorex Tutorial,2017.

[5] JunfengXie, et al, " A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," IEEE Communications Surveys & Tutorials, vol. 21, No. 3, Third Quarter 2019.

[6] https://www.pluralsight.com/guides/blockchain-architecture.

[7] Pinyaphat Tasatanattakool and Chian Techapanupreeda, "Blockchain: Challenges and Applications," International Conference on Information Networking (ICOIN) 2018, IEEE.

[8] Vitalik Buterin, "Ethereum and the Decentralized Future," Future Thinkers Podcast.2015-04-21.Retrieved 2016-05-13.

[9] Thomas and Syed Akram, " Blockchain Literature -review ," 2017 2nd IEEE Akanksha Kaushik, Archana Choudhary , Chinmay Ektare,Deepti, International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT),May19-20,2017,India.

[10] Kanika Agrawal, Mayank Aggarwal Sudeep Tanwar et al, "An Extensive Blockchain Based Applications Survey: Tools, Frameworks, Opportunities, Challenges, and Solutions," date of publication 3rd November 2022, date of current version 9th November 2022. DOI10.1109/ACCESS.2022.3219160.

[11] J. A. Stankovic. Research directions for the Internet of Things. IEEE, Internet of Things Journal,1(1):3–9,Feb2014.

[12] J.Lin, W.Yu, N.Zhang, X.Yang, H.Zhang, and W.Zhao.A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5):1125–1142, Oct2017.

[13] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang. "A survey on the edge computing for the Internet of Things". IEEE Access,6:6900–6919,2018.

[14] Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine and Rachid Benlamri, "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research," Appl. Sci. 2019, 9, 1736; doi:10.3390/app9091736 www.mdpi.com/journal/applsci.

[15] Ahmed Afif Monra, Olov Schelén(Member, IEEE), and Karl Anderson, (Senior Member, IEEE), "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities, " Received July 7, 2019, accepted July 28, 2019, date of publication August 19, 2019, date of current version September 4, 2019. Digital Object Identifier 10.1109/ACCESS.2019.293609 VOLUME 7, 2019.

[16] Rabab Jafri and Shikha Singh, "Blockchain applications for the healthcare sector: Uses beyond Bitcoin, in Blockchain Applications for Healthcare Informatics. https://doi.org/10.1016/B978-0-323-90615-9.00022-0.

[17] Omer F. Cangir, Onur Cankur, Adnan Ozsoy, "A taxonomy for Blockchain-based distributed storage technologies," Information Processing and Management 58, Elsevier, 10 May 2021.

[18] Jorge Lopes and Jose Luis Pereira, "Blockchain Technologies: Opportunities in Healthcare," Springer Nature Switzerland AG 2019 T. Antipova and A. Rocha (Eds.): DSIC 2018, AISC 850, pp. 435–442, 2019. https://doi.org/10.1007/978-3-030-02351-5_49.

[19] Meng Shen, Gaopeng Gou, and Qi Xuan, "Security and privacy of blockchain," Elsevier, Blockchain: Research and Applications, Volume 4, Issue 1, March 2023, 100130.