# A Blockchain Architecture for Secure Decentralized System and Computing

Sandhya Avasthi
*Department of CSE, ABES Engineering College*
Ghaziabad, UP (India)
sandhya_avasthi@yahoo.com

Khushboo Jain
School of Computer Science, UPES
Dehradun, UK, India
khushboojain2806@gmail.com

Ayushi Prakash
Department of CSE, AKGEC Engineering College
Ghaziabad, India
ayushi5edu@gmail.com

Tanushree Sanwal
KIET School of Management
KIET Group of Institutions Delhi-NCR, Ghaziabad, India
tanushree.sanwal@kiet.edu

***Abstract*— Recent growth in Internet infrastructure has increased demands for Internet technology and so there is a need for a secure decentralized system that is combined with secure and transparent infrastructure. Blockchain technology can store information in a distributed manner securely. Blockchain technology has expanded significantly over the past few years, with new applications and use cases being discovered and developed every day. The decentralized nature of blockchain, combined with its secure and transparent infrastructure, has made it a highly sought-after solution for various industries, including finance, healthcare, supply chain management, and government services. The expansion of blockchain technology is a result of its increasing adoption and integration into various sectors such as finance, healthcare, supply chain management, and more. One of the key drivers of the expansion of blockchain is the increasing demand for secure, tamper-proof, and transparent transactions. This has led to the development of various blockchain platforms, such as Ethereum, which helps in the development of decentralized applications or Apps for a variety of purposes from financial records to data storage.**

***Keywords*— *Smart Contract, Blockchain, Distributed System, P2P, contracts, censorship.***

## I. INTRODUCTION

As the digital era emerges, Blockchain technology has also gained popularity in recent years as a way to create secure, transparent, and decentralized systems. Blockchain is a distributed database or ledger of records distributed we can say that the copy of records is not in the centralized database instead of the centralized database the copy of the database is also available to all the nodes (i.e devices connected on the network) in such that the no changes are no possible in the records i.e it is immutable [1,2]. Blockchain has become popular with the advancement of Bitcoin which is an open-source online currency that is immutable. Everyone hears the word Bitcoin instead of Blockchain it is like that when we come to toothpaste we can call it Colgate instead of Toothpaste. The other popular blockchain-based E-Currencies are Bitcoin, Dogecoin, etc. There are many Blockchain networks available in the world in some popular ones are Ethereum [3,4]. Data and documentation will be accessible to the public and simple to verify because the blockchain functions as a decentralized distributed architecture without the need for a central authority. When used in the healthcare industry, the data blocks are not fully visible to the public; however, authorized individuals can read, retrieve, or verify them before they are approved for inclusion in the blockchain.

In this context, the discussion will provide an overview of the architecture for Blockchain technology, involving its key components that work together to support the development of a decentralized system with its advantages and disadvantages along with that there is also discussion of blockchain and smart contracts along with that we also learn how we can integrate blockchain into our web-based application. We will explore the network, the consensus, the data structure, and smart contracts components and challenges in that.

## II. DECENTRALIZED SYSTEM

A Decentralized System is a system of nodes or devices in which the data or ledger is not stored at a centralized server instead the data is shared over each node. Each node acts as a separate system with all records [See Figure 1]. As the data is stored across all nodes (i.e. Devices on the Network) it is not possible to temper any record for tempering we need to update data at each node which is not possible. It refers to the transfer of control and decision-making from a central authority to a decentralized authority [5].


Figure 1: Decentralized Architecture

### *A. Centralized System Vs Decentralized System*

The major differences between the Centralized System and Decentralized Systems are:

| Centralized System | Decentralized System |
|---|---|
| Maintained and controlled by a single entity hence easy to temper | It is not maintained or owned by a single entity hence difficult to temper. |
| Maintained and controlled through a central system | Data is added after consent from all nodes |

| | |
|---|---|
| Control through a central entity | No one owns that data and everyone owns the data |
| Yes | No |
| Low | Extremely High |
| Maintained and controlled through the central system | Increases when no of nodes increase |
| Maintained and controlled through the central system | Decreases when no of networks increases. |
| ERP System | Blockchain |

### *B. Merits & Demerits of Decentralized System*

The Merits of Decentralized System provides a trustless environment as each one has a copy of the database and improves data reconciliation. In addition, some other merits are reducing points of weakness, optimizing distribution, provides immutability, security, transparency, and full control over participating nodes [6-7]. Decentralized system protects data by utilizing encryption algorithms making it difficult for unauthorized users to tamper with data.

Some demerits of the Decentralized System are its cost, lack of consensus, clarity, and discipline. The overall implementation and maintenance cost is high due installation of separate hardware at each location. Also maintaining uniformity across various locations is challenging, a lot of variations are there in security practices [8].

## III. BLOCKCHAIN BACKGROUND

Blockchain technology became popular due to its secure nature in the case of the cryptocurrency Bitcoin, after the Bitcoin emergence Blockchain technology has taken a sharp turn.

### *A. What is Blockchain?*

Blockchain is a distributed immutable ledger where data is stored in the form of blocks for each new information or data a new block is created and also stores the hash of the previous block in such a way that it creates the chain of records [5,8]. Hence Blockchain is the composition of various Blocks that are linked together where each blocks consist of some data and some raw data like timestamps, previous hash, etc. In case when anyone changes the data in the ledger then that data is matched with the data stored in the different networks along the blockchain network and if the majority is in favor of that data is tempered then the changed data is replaced with the original data [9-10]. The Structure of the Blockchain Block is here depicted in Figure 2.

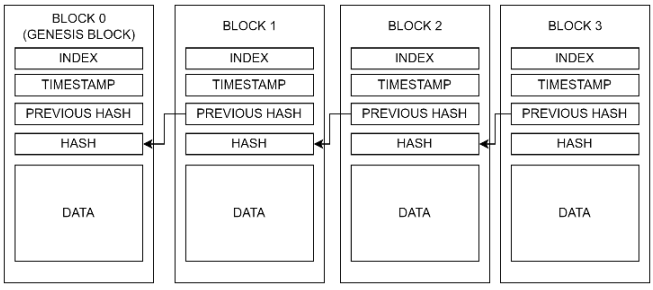


Figure 2: Structure of Blocks in Blockchain Network

There are mainly three types of *Blockchain Public Blockchain*, *Consortium Blockchain*, and *Private Blockchain*. In the case of Public Blockchain, all participants can verify transactions and can become part of the consensus process. Whereas in Private Blockchain participating nodes are kept restricted, not all nodes have authority on data access.

### *B. Structure of Blockchain*

The Structure of a Blockchain consists of the Blocks that are chained together regularly each block in the network stores the address of the previous block. The First Block in the Blockchain network is called as "Genesis Block" or "Block 0" as the Blockchain chain originates from here. The complete information regarding the structure of the Blockchain is also depicted in Figure 3.

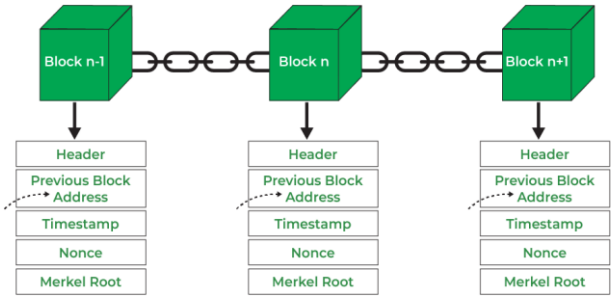


Figure 3: Structure of Blockchain

### *C. Requirements of Blockchain*

As the world moves towards the digital era the need for the database increases and the regular database is easy to modify because all the records are stored in the centralized storage which are in the same or different geographical area.

Due to data tempering everyone needs a trusted database which is impossible to temper and has no centralized storage so we move towards decentralized storage where data is not stored in the central server instead data is stored on each node means a copy of data is available to each node which means in case of any change the data is matched with the data available to other nodes which is close to impossible so blockchain prevents tempering of the data.

The main requirement of blockchain is to develop trusted data which is impossible to temper. In addition, Blockchain technology is useful for storing records such as educational documents, healthcare, the Internet of Things, and E-documents of all kinds.

### *D. Merits and Demerits of Blockchain*

The merits of Blockchain are Immutability and transparency. Blockchain supports concepts of *Immutability* which means the records are impossible to temper i.e. Blockchain prevents tempering of data within the blockchain network. Blockchain is transparent as the copy of records is available to all nodes available in the network.

The limitations/demerits of Blockchain are its speed, performance, cost, and data modifications.

- Speed and Performance: Blockchain is considerably slower than traditional databases as while working with records blockchain more operations are carried out which decreases speed on insertion of records [11]. Speed and performance are proportional to number of nodes in the network.

- Costly: Blockchain is costlier as compared with the traditional database as it requires proper planning and integration with blockchain.
- Data Modification: It is not easy to insert or update records in the blockchain for that we need to write codes or contracts which is time-consuming and expensive.

## IV. Smart Contracts

Smart Contracts are the programs stored in blockchain that automate the task of execution on agreement with predefined conditions that are set up when developing smart contracts. On the other hand, one can say that smart contracts are the authentication system of the blockchain which have predefined conditions that are first checked when a new block is inserted in smart contracts [12,13,14,15].

Smart Contracts are written through a programming language called "Solidity" which is an object-oriented language and licensed under GNU General Public License v3.0. Smart contracts also help automate the task of workflow, triggering the next action when specific conditions are met [15]. A sample Smart Contract for Todo List written in solidity is shown as follows:

```
pragma solidity >=0.7.0 <0.9.0;

contract Todos {
    struct Todo {
        string task;
        string timestamp;
        bool status;
    }
    mapping (address => Todo[]) private Users;

    function addTodo(string calldata _task,string
calldata _timestamp) external{
      Users[msg.sender].push(Todo({
          task: task,
          timestamp:timestamp,
          status:false
      }));
    }
```

## V. Blockchain Enabled Decentralized Systems

Blockchain is a way to store records in the form of a distributed ledger which develops the concept of a Decentralized System. Traditionally, a Centralized System was used which has certain disadvantages and certain limitations (i.e. No Data Immutability, Single Point of Failure, and Less tolerance), where there is a task of a central authority to control and manage the system. However, in a Blockchain-Enabled System or Decentralized System, there is no central system which means there is no single authority who manages and maintains the system and has no central point of control or data. In a Blockchain-powered Decentralized System, records are not stored on a central server instead records are stored on each node. In Blockchain, transactions are validated and recorded on a distributed ledger which is composed of multiple devices that are connected on the network called Nodes. Each node has a copy of the complete ledger and is validated by consensus among all the nodes.

The Decentralized Blockchain network has multiple benefits such as eliminating central authority or intermediaries such as Banks and other financial institutions which reduces running costs as well as increases efficiency provides increased transparency and security. The Decentralized System powered by Blockchain has the potential to transform traditional industries into modern Industries by creating new Business Models. The architecture of this system is global with capacity to deal with shutdowns and attacks very well. In addition, it is censorship-resistant which means nodes do not need permission to join peer-to-peer network.

For Example: Let's take the example of Decentralized Finance (DeFi) an Innovation in the field of Blockchain which creates an emerging path for Blockchain to take control over financial transactions. DeFi now emerged as the new paradigm in the finance industry, offering a range of financial services involving E-Currency, Crypto-Currency, etc. that are accessible to everyone regardless of Internet Connection, geographical location, and financial status. Other than financial services, Blockchain is also involved in Supply Chain Management, E-Voting, and Digital Identity Verification.

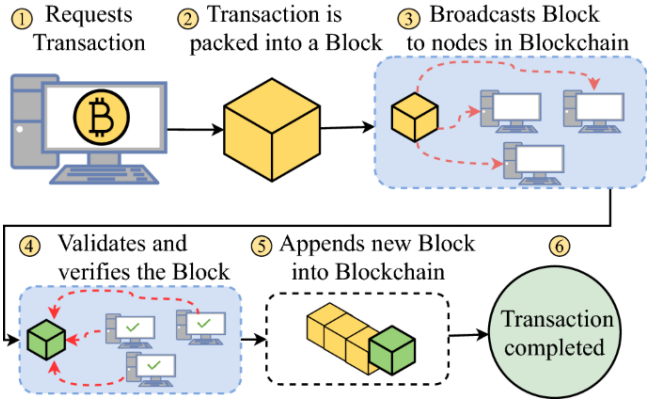


Figure 4: Process of Block Addition in Existing Blockchain

### A. *Role of Blockchain*

In a Decentralized System, Blockchain helps in creating records that are not on a central server instead they are the nodes (i.e Devices connected on the Blockchain Network) which means they are not handled by a central authority and Blockchain provides smart contracts that are generally the Programs that match the predefined conditions and on the basic of that condition the particular action is triggered. Every new record or block on the blockchain is proven to be authentic and digitally signed to ensure it is genuine. Before its addition to the blockchain, it should be verified by the majority of nodes in a network.

In Blockchain, the new Records can go through various phases involving validation. These are:

- A Transaction is requested
- A Block that represents the transaction is created.
- The Block is sent to every node in the network
- Nodes validate the transaction
- Node receives a reward for the proof of work
- The Block is added to the existing Blockchain
- The Transaction is complete.

### B. *Types of Blockchain Architecture*

Blockchain architecture may be implemented in three ways:

- Public Blockchain Architecture- Here, the data is available to the public who is willing to participate ex. Bitcoin and Ethereum follow public blockchain architecture.
- Private Blockchain Architecture- In this architecture, the data to only available to the members of the organization or any other person who is invited to the organization as a guest.
- Consortium Blockchain Architecture- In this architecture, the data is available to the public as well as to the users of an organization. This architecture is also used when there are multiple organizations where that can share their data.

### *C. Types of Decentralized Architecture*

The Blockchain follows one of the following levels of decentralization.

- **Fully Centralized**- These blockchain systems are entirely controlled and managed by a single central, authority
- **Semi-Decentralized**- These blockchain systems are managed and controlled by multiple authorities.
- **Fully Decentralized**- In this architecture, there is no central authority for the management.

### *D. Requirements of System*

The main reasons for the requirements of the Blockchain Enable Decentralized System are:

- Immutability: Everyone wants Immutable data which means that data is authentic and did not change by anyone thus Blockchain Enables Decentralized System is the solution for that. It prevents data tampering as all blocks are connected in a chain and case of tampering chains are disturbed another one is that each node on the blockchain network has a copy of the data and in case of tampering the data is recovered to the authentic data through the concept on consensus protocol of blockchain.
- Transparency: Blockchain increases transparency in the data as data is available to all the nodes in the network which means anyone within the network can view the data as per their access. So Blockchain enables Decentralized systems are also required to increase transparency in the data.
- Single Point of Failure: Blockchain enables a Decentralized System and also reduces the single point of failure as the data is not accessed through a single point or central server.
- Fault Tolerance: Blockchain enables a Decentralized System to be very fault-tolerant as there is no dependence on the central server and there is no load on the central server instead loads are split into the nodes or devices connected to the network.

### *E. Pros. and Cons. of System*

**Pros of Blockchain-Enabled Decentralized System:**

- These Systems prove the authenticity of the data which means that the Data stored in these are authentic and are tamper proof.
- These systems have no Single Point of failure due to the absence of the central server.
- These Systems have maximum Fault Tolerance as each node on the network has its hardware and there is no dependence on the infrastructure of the central system
- The data in this system are transparent as data is available to every node on the network.

**Cons of Blockchain-Enabled Decentralized System:**

- These Systems have limited Speed and Performance which means speed and performance are inversely proportional to no of nodes on the network as when no of nodes increases the speed and performance decrease and vice versa.
- The cost of setup of these systems is high as compared to the central system.
- Each operation in this system takes time to execute as it has gone through various smart contracts.
- Blockchain has limited scope as further research is going on it.

## VI. Architecture For Blockchain Enabled Decentralized System

The architecture of the blockchain technology comprises of distributed network of nodes (i.e network created by connecting multiple devices or nodes) that work together to validate and record transactions on the blockchain ledger along with these devices there are there are some programs needed for validation of conditions known as smart contracts. This architecture enables decentralized systems to be built, as no single entity or node has access to the whole network. As per the core fundamentals, blockchain architecture consists of three main components; the network, the consensus mechanism or protocol, and the data structure needed to store the blocks.

### *A. The Network:*

The network components or the setup generated by connecting multiple devices or nodes to form the decentralized network. These nodes can work together to ensure that the blockchain remains secure, transparent, and tamper-proof.

### *B. The Consensus Protocol:*

The Consensus protocol or mechanism ensures that all the nodes on the network have the current state of the blockchain which is achieved by various algorithms that come under consensus protocol such as Proof of Work (PoW), Proof of stake (PoS), and Delegated Proof of stake (DPoS).

### *C. The Data Structure:*

The data structure of the blockchain deals with the storage of the transactions records of the transaction that took place on the network. Each Block of the Blockchain consists of information about the set of transactions, along with a unique cryptographic hash that contains the reference to the previous block which leads to the chain of blocks In other way we can say that Blockchain starts with “Block 0” or “Genesis Block” upto “Block N” where each block stores the reference to the previous block which means each n block consists of the reference to n-1 block that creates the chains of records.

In addition to these core components i.e. the network, the consensus protocol, and data structure. Blockchain

architecture also includes smart contracts (the self-executing contracts the type of agreement between parties written in the form of code using Solidity Programming Language). Smart Contracts allow the automation of complex transactions and can be programmed to execute triggers based on a specific condition.

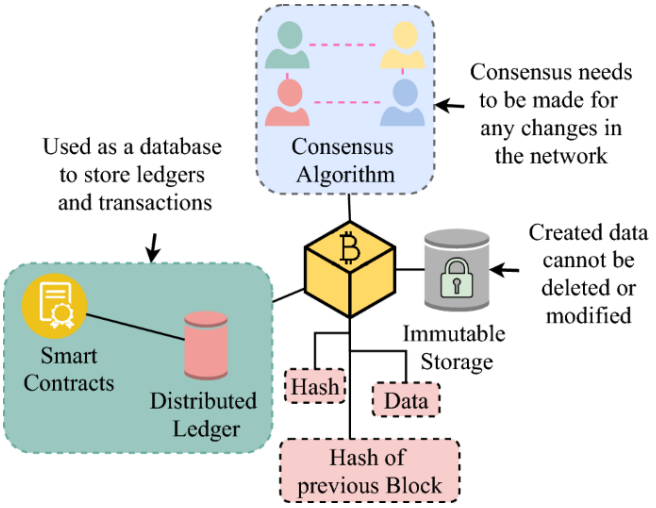


Figure 5: Core Components of Blockchain

Overall, the architecture of blockchain development of transparent, tamper-proof decentralized system. By leveraging a distributed network of nodes, a consensus mechanism, and a tamper-proof data structure with the potential to create innovations.

For the development of decentralized systems using Blockchain, we must go to the mentioned steps:

1. Choose the Blockchain Platform: The First step in the development is to choose a blockchain platform from available blockchain platforms i.e. Ethereum, Hyperledger, and EOS, etc. among those available choose that platform that suits system requirements.
2. Develop Smart Contracts: The next step is to develop smart contracts using solidity here we have to develop a smart contract that governs our app functionality.
3. Create a Decentralized Application (DApp): Develop an app that can work with smart contracts and allow users to execute system functionality.
4. Define User Roles: here we have defined the access-based user roles.
5. Integrate with a cryptocurrency: To make system functionalities work properly we need to connect our app with a cryptocurrency such as Ether or Bitcoin.
6. Publish the DApp: To make the System accessible to everyone we need to publish the app on the chosen platform.
7. Data Audit: As Blockchain is highly secure we must take regular audits of the data and use encryption and other privacy-enhancing technologies to protect user data.

## VII. Blockchain Enables Decentralized System Development And Challenges

As discussed above in this review paper, a Blockchain enabled Decentralized System can develop a system that provides a way to record and verify transactions securely and transparently. Decentralized Mode is achieved by connecting the multiple machines on a network which helps in validation and recording of transactions.

One of the major advantages of Decentralized Systems based on Blockchain technology is that they are free from censorship and control by a single authority or government as nodes ensure that no single node has complete access to the blockchain network. A decentralized system provides a way to store data in a secure environment that can be accessed through necessary permissions [11-15].

However, there are various challenges in this Blockchain-based Decentralized journey. One of the popular is Scalability as the current blockchain can only handle a limited number of transactions within seconds making a blockchain decentralized system take control over a centralized system which can handle millions of transactions within seconds. Another challenge associated with the Blockchain Decentralized System is the Lack of Interoperability which means adoption and integration of that in various industries and platforms. Along with that, there is also the challenge of Government regulations as the development of regulations also makes adoption slow.

Overall, while blockchain technology helps in the development of a decentralized system which has its various advantages, there are still several challenges that need to be addressed to fully realize the potential of this technology, Further research is going on Blockchain which helps in creating a backdoor in the adoption of Blockchain technology in various fields including E-Voting, Supply Chain Management, Academic Records Management etc.

## VIII. Future Of Blockchain Enables Decentralised System

The Future of Blockchain technology and its ability to develop decentralized systems is promising. These continue to maturity by providing better solutions to some of the sectors where they can make a significant impact. One area where Blockchain Technology can make a significant impact is the Financial Sector which is one of the crucial sectors involving records with money transactions entry which must be temper proof [3, 17]. Decentralized Finance (DeFi) applications which are built on blockchain technology have already emerged, enabling P2P lending, and trading without the need of a central authority or financial institutions [18,19]. Another area where Blockchain makes a huge impact is “Supply Chain Management” involving management of the records related to the supply of goods. It increases transparency, reduces fraud, and improves the efficiency of the supply.

Other areas where Blockchain creates a huge impact are Online Voting, Academic Records Management, etc. Blockchain technology also be used to develop a decentralized identity system that enables individuals to take control of personal data and protect their privacy online more

information about the future use of blockchain technology is depicted in Figure 6.

The future of Blockchain includes integration of it with IoT, Artificial Intelligence, and Machine Learning to keep records tamperproof. These technologies can leverage the decentralized and secure nature of blockchain to develop innovative solutions for various industries.

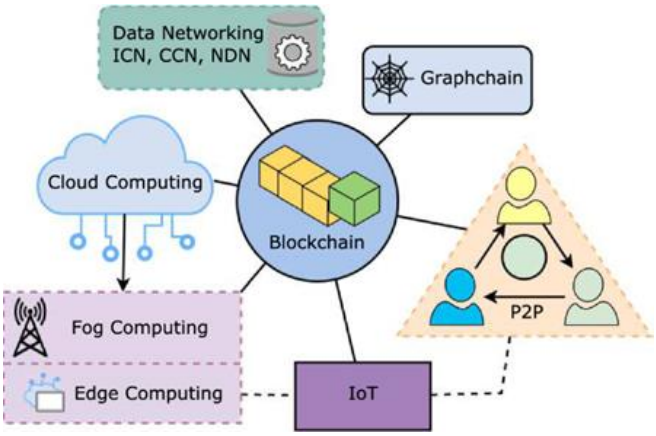


Figure 6: Future of Blockchain-Enabled Decentralized System

## CONCLUSION

In conclusion, we can say that blockchain technology has the potential to change the way we build decentralized systems, by providing transparent and tamper-proof management of records and preventing the censorship of records as well as management by a signal central authority or Government. Decentralized Systems powered by Blockchain have the potential to transform industries involving finance, education, voting, supply chain management, and identity management by developing transparency and reducing fraud. Such powerful system leads to the trust building that records are authentic paving way for Web 3.0. The existing challenges as discussed in this research can be handled shortly as research is going on the blockchain. Overall, the potential benefits linked with Blockchain technology and decentralized systems are significant and it is an exciting time for developers to leap into it by exploring different opportunities and developing world-changing innovations.

## REFERENCES


[1] R. Kumar, L. Badwal, S. Avasthi and A. Prakash, "A Secure Decentralized E-Voting with Blockchain & Smart Contracts," 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2023, pp. 419-424, doi: 10.1109/Confluence56041.2023.10048871.

[2] X. Zhao, Z. Lei, G. Zhang, Y. Zhang, and C. Xing. "Blockchain and distributed system." In *Web Information Systems and Applications: 17th International Conference, WISA 2020, Guangzhou, China, September 23–25, 2020, Proceedings 17*, pp. 629-641. Springer International Publishing, 2020.

[3] S. Zhang, and Dongzhi Cao. "A blockchain-based provably secure anonymous authentication for edge computing-enabled IoT." *The Journal of Supercomputing* (2023): 1-31.

[4] B. Zaabar, O. Cheikhrouhou, Faisal Jamil, Meryem Ammi, and Mohamed Abid. "HealthBlock: A secure blockchain-based healthcare data management system." *Computer Networks* 200 (2021): 108500.

[5] S. Rouhani and R. Deters. "Security, performance, and applications of smart contracts: A systematic survey." *IEEE Access* 7 (2019): 50759-50779.

[6] T. Kim, J. Ochoa, T. Faika, H. A. Mantooth, J. Di, Qinghua Li, and Young Lee. "An overview of cyber-physical security of battery management systems and adoption of blockchain technology." *IEEE Journal of Emerging and Selected Topics in Power Electronics* 10, no. 1 (2020): 1270-1281.

[7] S. Avasthi, R. Chauhan, and D. P. Acharjya. "Techniques, applications, and issues in mining large-scale text databases." In *Advances in Information Communication Technology and Computing: Proceedings of AICTC 2019*, pp. 385-396. Springer Singapore, 2021.

[8] S. Avasthi, R. Chauhan, and D. P. Acharjya. "Topic modeling techniques for text mining over a large-scale scientific and biomedical text corpus." *International Journal of Ambient Computing and Intelligence (IJACI)* 13, no. 1 (2022): 1-18.

[9] H. L. Pham, T. H. Tran, T. D. Phan, V.T. D. Le, D. K. Lam, and Y. Nakashima. "Double SHA-256 hardware architecture with compact message expander for bitcoin mining." *IEEE Access* 8 (2020): 139634-139646.

[10] S. Zhang, & J. H. Lee. Analysis of the main consensus protocols of blockchain. ICT Express, 6(2), 2020, pp. 93-97.

[11] S. Avasthi, T. Sanwal, S. Sharma, & S. Roy. VANETs and the Use of IoT: Approaches, Applications, and Challenges. Revolutionizing Industrial Automation Through the Convergence of Artificial Intelligence and the Internet of Things, 2023, pp. 1-23.

[12] Idelberger, F., Governatori, G., Riveret, R., & Sartor, G. (2016, July). Evaluation of logic-based smart contracts for blockchain systems. In International symposium on rules and rule markup languages for the semantic web (pp. 167-183). Springer, Cham.

[13] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.Y. Wang. "Blockchain-enabled smart contracts: architecture, applications, and future trends." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49, no. 11 (2019): 2266-2277.

[14] R. Chauhan, S. Avasthi, B. Alankar, and H. Kaur. "Smart IoT systems: Data analytics, secure smart home, and challenges." In *Transforming the Internet of Things for Next-Generation Smart Systems*, pp. 100-119. IGI global, 2021.

[15] Khan, Shafaq Naheed, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. "Blockchain smart contracts: Applications, challenges, and future trends." *Peer-to-peer Networking and Applications* 14 (2021): 2901-2925.

[16] S. Avasthi, R. Chauhan, S. L. Tripathi, and T. Sanwal. "COVID-19 research: Open data resources and challenges." In *Biomedical Engineering Applications for People with Disabilities and the Elderly in the COVID-19 Pandemic and Beyond*, pp. 93-104. Academic Press, 2022.

[17] M. Varshney, M. Yadav, M. Bisht, K. Choudhary, S. Avasthi. "Detecting Object Defects for Quality Assurance in Manufacturing." In *International Conference on Advances in IoT and Security with AI*, pp. 347-357. Singapore: Springer Nature Singapore, 2023.

[18] J. Zarrin, H. W.Phang, L. B. Saheer, and B. Zarrin. "Blockchain for decentralization of internet: prospects, trends, and challenges." *Cluster Computing* 24, no. 4 (2021): 2841-2866.

[19] S. Avasthi, T. Sanwal, A. Prakash, and S. L. Tripathi. "A Study of Multimodal Colearning, Application in Biometrics and Authentication." *Multimodal Biometric and Machine Learning Technologies: Applications for Computer Vision* (2023): 103-128.