**SYNOPSIS**

**Report on**

**Comparative Study of Consensus Algorithms**

**by**

Riya Mudgal

2000290140105

**Session:2021-2022 (4th Semester)**

Under the supervision of

**Prof. (Dr.) Arun Kumar Tripathi**

Co-supervisor

**Mr. Apoorv Jain (BlockChain developer)**

### KIET Group of Institutions, Delhi-NCR, Ghaziabad



### Department Of Computer Applications

**KIET GROUP OF INSTITUTIONS, DELHI-NCR, GHAZIABAD-201206**

(march- 2022)

**ABSTRACT**

BlockChain is the world’s most trusted service. It serves as a ledger that allows transaction to take place in a decentralized manner. There are so many applications based on BlockChain technology, including those covering numerous fields like financial services, non-financial services, internet of things (IoT), and so on. BlockChain combines a distributed database and decentralized ledger without the need of verification by central authority. This chapter surveys the different consensus algorithms, BlockChain challenges, and their scope. There are still many challenges of this technology, such as scalability and security problems, waiting to be overcome. The consensus algorithms of BlockChain are proof of work (POW), proof of stake (POS), ripple protocol consensus algorithm (RPCA), delegated proof of stake (dPOS), stellar consensus protocol (SCP), and proof of importance (POI). This chapter discusses the core concept of BlockChain and some mining techniques, consensus problems, and consensus algorithms and comparison algorithms on the basis of performance.

KEYWORDS: [ BlockChain, Smart Contract, Proof of Work, Proof of stake, Ripple Protocol, Delegated Proof of Stake]

**TABLE OF CONTENTS**

1. Introduction 4
2. Literature Review 5-6
3. Project / Research Objective 7
4. Research Methodology 8
5. Project / Research Outcome 9
6. Proposed Time Duration 10

References 11

1. **INTRODUCTION**

A BlockChain can be interpreted as a distributed database that incorporates every event or transaction, executed and shared amongst the concerned parties. Each transaction is vehemently verified and once an information is entered, it can never be erased without the consent of the involved parties.

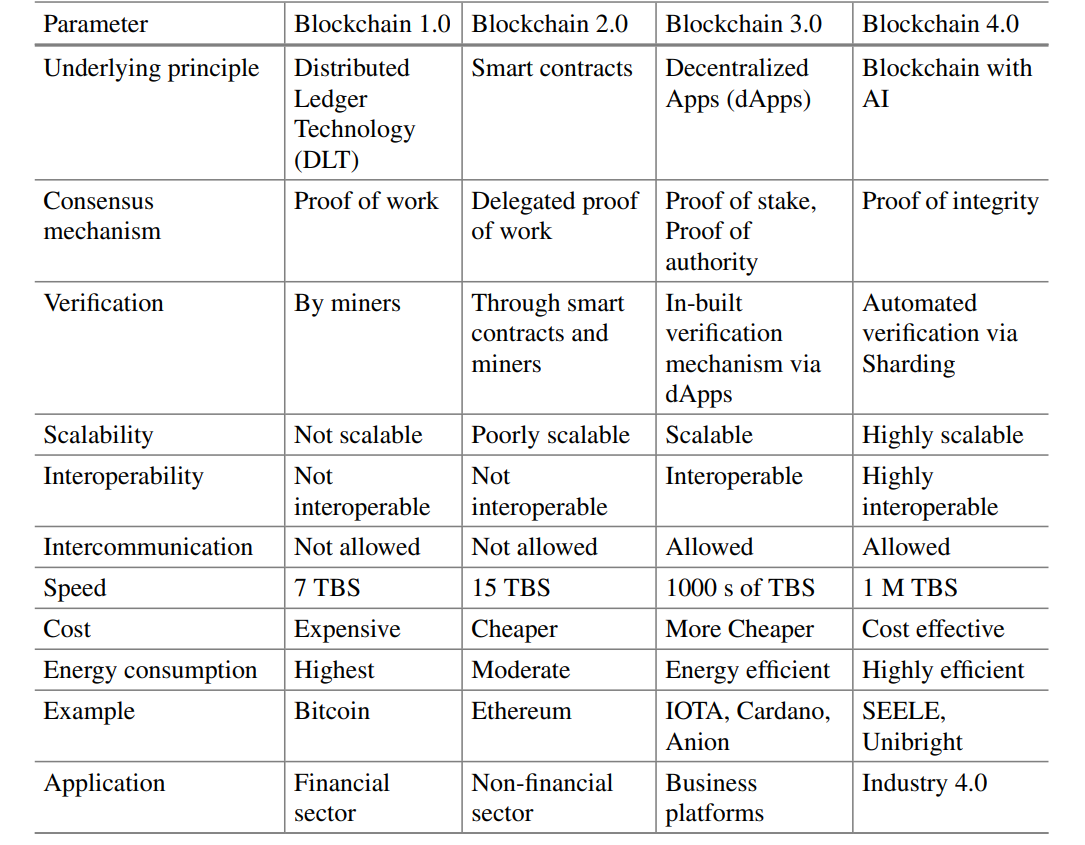
BlockChains are thus like public registers where every transaction is accumulated as a series of blocks. They are essentially based on the concept of Cryptography and Distributed Systems. Each successive block stores the hash of the its preceding block. Thereby, if any modification is made into the previous block, its corresponding hash is modified and hence here is a mismatch with the one stored in the successive block. This features makes BlockChain tamperproof and the contaminated block can be easily identified.

Also BlockChains eliminate the need of any central authority for any kind of validation. Another important feature of BlockChain is its distributed nature where its several copies are stored by different parties over different networks which makes any modification quite tedious and further enhances the security of BlockChains.

1. **LITERATURE REVIEW**

BlockChain is a main technology for different cryptocurrencies. Today BlockChain has main research interest in the field of security due to its features like, stability, security, inalterable and decentralization.

* 1. **Evolution of BlockChain**



* 1. **Consensus Algorithms**

In BlockChain technology, the transactions can be done securely with the help of consensus algorithms in a distributed system which has P2P connections of blocks, without interference of mediator. So the consensus algorithms are playing a key role for preserving the security and integrity of a distributed network in BlockChain technology. It is basically used for maintaining the trust in BlockChain technology.

The consensus algorithms are divided into two types, proof based and voting based, that are going to be discussed in Project/Research Objective.

1. **PROJECT/RESEARCH OBJECTIVE**

To date, many variants of proof-based consensus algorithms have been proposed, which are based on PoW, PoS, their hybrid form, and other variants that are made independently from these two major ones. The basic concept of proof-based consensus algorithm is that among many nodes joining the network, the node that performs sufficient proof will get the right to append a new block to the chain, and receive the reward.

In order to execute the voting based consensus algorithm, the nodes inside the verifying network should be known and adjustable, so that they can exchange the message easier. This is the main. difference compared to proof-based consensus algorithms, which nodes are often free to join and withdraw from the verifying network. Also, in voting-based consensus algorithm, besides maintaining the ledger, all the nodes in the network would have to verify together the transactions or blocks. They will communicate with others, before deciding to append their proposed blocks to their chain or not

1. **RESEARCH METHODOLOGY**

Referencing research papers on BlockChain, smart contracts, and consensus algorithm

The main idea behind this paper is to give a simplified view of various Consensus Algorithms

1. **PROJECT/ RESEARCH OUTCOME**

The outcome of this paper would be a research paper covering following topics:

1. BlockChain Evolutions

2. Various Consensus Algorithms

3. Comparative Study of Various Consensus Algorithms

then submitting a modified version of this paper in Scopus Journal

1. **PROPOSED TIME DURATION**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Week 1 | Week 2 | Week 3 | Week 4 | Week 5 | Week 6 | Week 7 | Week 8 |
| Feasibility Study |  |  |  |  |  |  |  |  |
| Research work |  |  |  |  |  |  |  |  |
| Paper writing |  |  |  |  |  |  |  |  |
| Implementation |  |  |  |  |  |  |  |  |

1. **REFERENCES**

1. https://en.wikipedia.org/wiki/Ledger

2. https://en.bitcoin.it/wiki/Block

3. <https://en.bitcoin.it/wiki/Genesis_block>

4. <https://en.wikipedia.org/wiki/Digital_currency>

5. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei,W., Qijun, C.: A review on consensus algorithm of BlockChain. In 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 2567–2572. IEEE (2017)

6. Norman, M.D., Karavas, Y.G., Reed, H.: The emergence of trust and value in public BlockChain networks. In: IX International Conference on Complex Systems, p. 22 (2018)

7. [Public Vs. Private BlockChain : A Comprehensive Comparison (BlockChain-council.org)](https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/)