COMPARATIVE STUDY OF BLOCKCHAIN MINING

A Thesis Submitted
In Partial Fulfilment of the
Requirementsfor the Degree of

MASTER OF COMPUTER APPLICATIONS

By
Riya Mudgal
(University Roll No. 2000290140105)

Under the Supervision of
Dr. Arun Kumar Tripathi
Professor

DR A.P.J. ABDUL KALAM TECHNICAL UNIVERSITY, UTTAR PRADESH
योगः कर्मसु कौशलम्
LUCKNOW

Submitted to

DEPARTMENT OF COMPUTER APPLICATIONS

KIET Group of Institutions,
GhaziabadUttar Pradesh-201206

(JUNE 2022)

CERTIFICATE

Certified that **RIYA MUDGAL 2000290140105** have carried out the project work having "**Comparative Study ho Blockchain Mining**" for Master of Computer Applications from Dr. A.P.J. Abdul Kalam Technical University (AKTU**)** (formerly UPTU), Technical University, Lucknow under my supervision. The project report embodies original work, and studies are carried out by the student himself / herself and the contents of the project report do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Date:

Riya Mudgal
(2000290140105)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date:

Prof. (Dr.) Arun Kumar Tripathi

Professor
Department of Computer Applications
KIET Group of Institutions, Ghaziabad

Signature of Internal Examiner **Signature of External Examiner**

Dr. Ajay Shrivastava
Head, Department of Computer Applications
KIET Group of Institutions, Ghaziabad

ABSTRACT

Blockchain's first implementation attention is crypto-currency. In this new distributed architecture, which is decentralized and has no central authority, Blockchain serves as an immutable distributed ledger for processing transactions with the participation of untrusted parties. Smart contracts allow states to be shared and transactions to be executed by participants in this decentralized network. Blockchain applications are crypto-currency based online wallets, Internet of Things, springing up, financial services, risk management, reputation system, etc. This paper aims to share knowledge on the growing importance of Blockchain technology in real-world applications. Furthermore, this paper provides a comparison of typical consensus algorithms for security aspects as part of Blockchain core components and technologies. According to this comparison and Blockchain applications, alternative Merkel tree based Blockchains are available in the market for faster and more secure transactions.

Blockchain is an immutable, transparent, public ledger that is distributed among the nodes in the network. It is a decentralized system in which transactions run on untrusted devices. To ensure equality and fairness, these transactions need to agree on some protocols. They are known as consensus algorithms. They are the core of Blockchain and decide how Blockchain works. Applying these algorithms, it is almost impossible for unauthorized users to crack the confidential information in the blocks. However, there are some security and performance issues that are required to be improved. In this paper, we have an overlook on various consensus algorithms, their working and where they are applied. In addition, we have reviewed Blockchain technology, its application areas, advantages, and issues.

Blockchain algorithms can be categorized into two main groups. The first group is proof-based consensus, in order to be included in the verifying network, nodes must qualify themselves as more qualified than their peers. The second group is voting-based consensus, to verify a new block or transaction, each node in the network must share their results before making a final decision. This paper provides a review of some Blockchain consensus algorithms that have been researched and that are currently being applied to some well-known applications**.**

ACKNOWLEDGEMENTS

Success in life is never attained single handedly. My deepest gratitude goes to my thesis supervisor, **Prof. (Dr.) Arun Kumar Tripathi** for his guidance, help and encouragement throughout my research work. Their enlightening ideas, comments, and suggestions.

Words are not enough to express my gratitude to Dr. Ajay Kumar Shrivastava, Professor and Head, Department of Computer Applications, for his insightful comments and administrative help at various occasions.

Fortunately, I have many understanding friends, who have helped me a lot on many critical conditions.

Finally, my sincere thanks go to my family members and all those who have directly and indirectly provided me moral support and other kind of help. Without their support, completion of this work would not have been possible in time. They keep my life filled with enjoyment and happiness.

Riya Mudgal

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

The concept of digital currency was first presented by Nakamoto. These cryptocurrencies are based on the concept of decentralization, and they are produced by a technology called the Blockchain. It is a disruptive and revolutionary technology of the 21st century. Bitcoin was believed to be a Blockchain by all communities in the world at first, but many myths swirled around the technology and its use in businesses. In the later stages, the core technology behind Bitcoin had a direct impact on researchers' perceptions of considering Bitcoin as Blockchain.

A Blockchain is a database that stores information electronically in digital form. By using a Blockchain, a record of data is guaranteed to be accurate and secure, and trust is generated without the need for a third party.

The fundamental difference between a traditional database and a Blockchain is how the data is structured. In a Blockchain, information is gathered together into groups called blocks, each of which holds a set of information. Once a block is filled with data, it is connected with the previously filled block, forming a chain of data known as a Blockchain. Blockchain is a decentralized, peer-to-peer (P2P) network and distributed in nature. Throughout the network, all participants can control it. Several computers are connected together to create the Blockchain network, and no changes to the block can be made without the network's consent. Data blocks can be considered containers for data. In a Blockchain network, the computers are called nodes, and every node has a copy of the digital ledger.

The block is a collection of data that contains transaction details like the timestamp and the link to the previous block generated by a hash algorithm. Each block is composed of two components: block header and block body.

The key features of a Blockchain are consensus, distributed computation, immutability, and authentication. Blockchains are too diverse to be used for all applications since they are a budding technology. In addition to tracking orders, payments, accounts, production and more, a Blockchain network can track many other things as well.

1.2 History and Evolution of Blockchain

- **1991-2008: Early Years of Blockchain Technology**

It was in 1991 that Stuart Haber and W Scott Stornetta envisioned what we call Blockchain today. In their first project, they worked on a cryptographically secure chain of blocks where time stamps of documents could not be tempered. They upgrade the system in 1992 to include Merkle Trees, which improves efficiency by allowing the collection of more documents on one block.

It is recognised that Satoshi Nakamoto, he could be an individual or a team of individuals that worked on Bitcoin, the first application of digital ledger technology. The first Blockchain was conceptualized by Nakamoto in 2008, and the technology has evolved and since then it has been used in a wide range of applications beyond cryptocurrencies.

- **2008-2013: Blockchain 1.0: Bitcoin Emergence**

  As the first application of Blockchain technology, Bitcoin was created in 2008. As described in Satoshi Nakamoto's whitepaper, Bitcoin is an electronic peer-to-peer network. Nakamoto created a genesis block from which other blocks could be mined, culminating in one of the largest chains of blocks that carried different types of information and transactions. In this way, Blockchain history contains a long list of applications resulting from the development of the technology.

- **2013-2015: Blockchain 2.0: Ethereum Development**

Vitalik Buterin, one of the first contributors to the Bitcoin codebase, is among a growing list of developers who believe that Bitcoin has not yet reached its full potential when it comes to leveraging the full capabilities of Blockchain technology. Buterin was concerned about Bitcoin's limitations, so he began to develop what he envisioned would be a malleable Blockchain that would also function as a peer-to-peer network.

In order to distinguish Ethereum from Bitcoin Blockchain, Buterin added the ability to record other assets such as slogans and contracts. With the new feature, Ethereum expanded its functionality from that of a cryptocurrency to a platform for developing decentralized applications.

- **2018: Blockchain 3.0: The Future**

Blockchain history and evolution go far beyond Ethereum and Bitcoin. There are new projects that seek to improve Bitcoin and Ethereum's shortcomings as well as add new features that leverage Blockchain technology.

There are a number of new Blockchain applications, such as NEO, billed as the first open-source, decentralized, and Blockchain platform in China.

Developers were racing to accelerate the Internet of Things so they used Blockchain technology to accelerate the process and came up with IOTA as a result.

Besides IOTA and NEO, other second-generation Blockchain platforms also have a ripple effect in the sector.

- **2015: Hyperledger**

Linux Foundation unveiled an open-source Blockchain umbrella project in 2015. They named the project as Hyperledger, and it acted as a platform for collaborative development of distributed ledger technology. In the context of global business transactions, Hyperledger seeks to improve systems' reliability and performance by making use of Blockchain technology.

1.3 Architecture of Blockchain

Blockchains provide a peer-to-peer distributed ledger method for secure and reliable transaction management. A ledger is an interconnected block in a structure that has other blocks interlinked with it. A distributed approach is used to share the databases. Every block is associated with a reference to the previous block via a timestamp server that controls the databases.

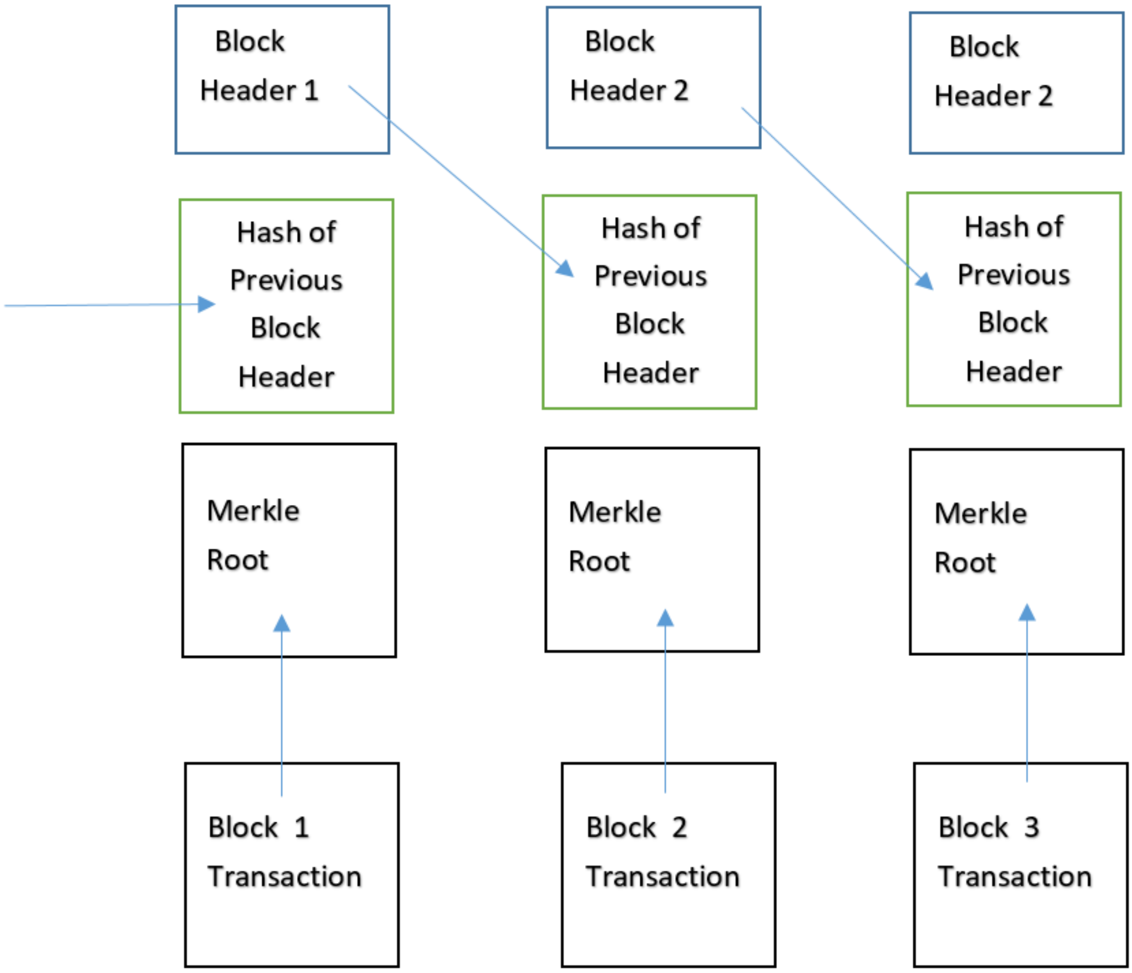


Fig 1.1: Block structures in Blockchain

1.4 Blocks in Blockchain

Blocks are the basic building blocks of Blockchain. The block represents a place on a Blockchain where information is encrypted and stored. Each block contains a header that verifies its validity. It contains metadata describing the block. Following information is stored as meta data:

a) Version filed: Which describes the current version of the block.

b) Previous block header hash: References the previous block's parent block.

c) Merkle root: Cryptographic hash of all transactions involved in this block.

d) Nonce: number of times the process repeated so that it becomes a complex task

1.5 How does a Blockchain work

Blockchain is intended to allow the recording and distribution of digital information without editing, this leads to immutable ledgers or records of transactions that cannot be altered, deleted, or destroyed. As a result, Blockchains are also referred to as distributed ledger technologies (DLT).

Below is the transaction process of Blockchain:

1. Transaction is entered
2. Transaction is then transmitted to a network of peer to peer computers scattered across the world
3. This network of computer then solves equations of puzzles to confirm the validity of the transaction
4. Once confirmed to be legitimate transactions, they are clustered together into blocks.
5. These blocks are then chained together creating a long history of the transaction that are performed
6. The transaction is completed

1.6 Distributed Ledger Technology

Distributed Ledger Technology (DLT) refers to the technological infrastructure and protocols that allows simultaneous access, validation, and record updating in an immutable manner across a network that's spread across multiple entities or locations.

Distributed ledger technology (DLT) refers specifically to the technological infrastructure and protocols that allow the simultaneous access, validation and updating of records that characterizes distributed ledgers. It works on a computer network spread over multiple entities or locations.

DLT uses cryptography to securely store data, cryptographic signatures and keys to allow access only to authorized users.

The technology also creates an immutable database, which means information, once stored, cannot be deleted and any updates are permanently recorded for posterity.

DLT has great potential to revolutionize the way governments, institutions, and corporations work. It can help governments with tax collection, the issuance of passports, recording land registries and licenses, and the outlay of Social Security benefits as well as voting procedures. The technology is making waves in industries such as finance, music and entertainment, diamond and other precious assets, art, supply chains of various commodities, and more.

1.7 How are Blockchains used in various fields

There are more than 10,000 other cryptocurrency systems that utilize Blockchain technology today. However, Blockchain is proving to be a reliable method for storing data about other types of transactions as well.

Walmart, Pfizer, AIG, Siemens, and Unilever are among the companies that have already incorporated Blockchain into their operations. For example, to help in tracing food products' journeys to their locations, IBM has created its Food Trust Blockchain. One form of Blockchain implementation is depicted here, but there are many others, discussing below.

1. **Banking and Finance**

   Banks can complete consumer transactions within 10 minutes if they integrate with Blockchain technology, here block creation times are constant regardless of holidays or the time of day or week. Furthermore, Blockchain provides banks with a more secure and swift way of transferring funds between institutions.

2. **Currency**

   Cryptocurrencies like Bitcoin are built on the Bl1.1ockchain. Due to the distributed nature, Blockchain allows Bitcoin and other cryptocurrencies to operate without a central authority. As a result, not only risk is reduced, but many of the transaction and processing fees are eliminated as well.

3. **HealthCare**

   Using Blockchain, healthcare organizations can securely store patients' medical records. The evidence and confidence that an individual's medical record cannot be altered can be provided by the Blockchain when a medical record is generated and signed.

4. **Smart Contracts**

   Smart contracts are computer code that can be incorporated into the Blockchain, facilitating, verifying, or negotiating contract agreements. A smart contract operates under a set of conditions that are agreed to by the participants. As soon as those conditions are met, the agreement is automatically enforced.

5. **Voting**

   A voting system based on Blockchain could prove useful. As demonstrated in the November 2018 midterm elections in West Virginia, voting with Blockchain could eliminate election fraud and boost voter turnout. By using Blockchain in this manner, votes would be virtually impossible to alter.

1.8 Benefits of Blockchain

Comparing with traditional data structure, what all we need to change are listed below:

Duplicate record keeping and third-party validations waste operations' time. Fraud and cyberattacks can occur in record-keeping systems. Limited Transparency. These factors slow business and drain profits. Therefore, we need a better method. To resolve all these problems, Blockchain came into existence having the following positive aspects:

1. **Enhanced security**

   We know how important it is to protect our crucial data and Blockchain can make a huge difference in how it is viewed. With its ability to create a record that cannot be tampered with and is encrypted from beginning to end, Blockchain prevents fraud and unauthorized activity. On the Blockchain, privacy issues can also be addressed by anonymizing data and ensuring access is controlled through permissions.

2. **Greater Transparency**

   Each organization has to maintain a separate database without Blockchain. As Blockchain uses a distributed ledger, transactions and data are recorded across multiple locations in an identical way. The same information is accessible to everyone with permissioned access, ensuring full transparency. All transactions are immutably recorded and dated and timestamped.

3. **Instant Traceability**

   In a Blockchain, the provenance of an asset is documented at every step along its journey. Blockchain facilitates direct sharing of provenance data with customers. In addition, traceability data can reveal weaknesses in supply chains. For example, goods may sit on a loading dock awaiting delivery.

4. **Increased efficiency and speed**

   Weak paper-based processes are time-consuming, likely to cause human error, and often need to be mediated by third parties. Transactions can be completed faster and more efficiently by automating these processes with Blockchain. A Blockchain can store and track documentation, as well as transaction details, eliminating the need of paper paperwork.

5. **Automation**

   It is even possible to automate transaction processes using "smart contracts," which increases efficiency and speeds the process even more. A transaction or process is automatically triggered when certain conditions are met. Smart contracts can be verified more easily, without human intervention, and without relying on third parties.

1.9 Types of Blockchain Networks

Following are the ways in which a Blockchain network can be build:

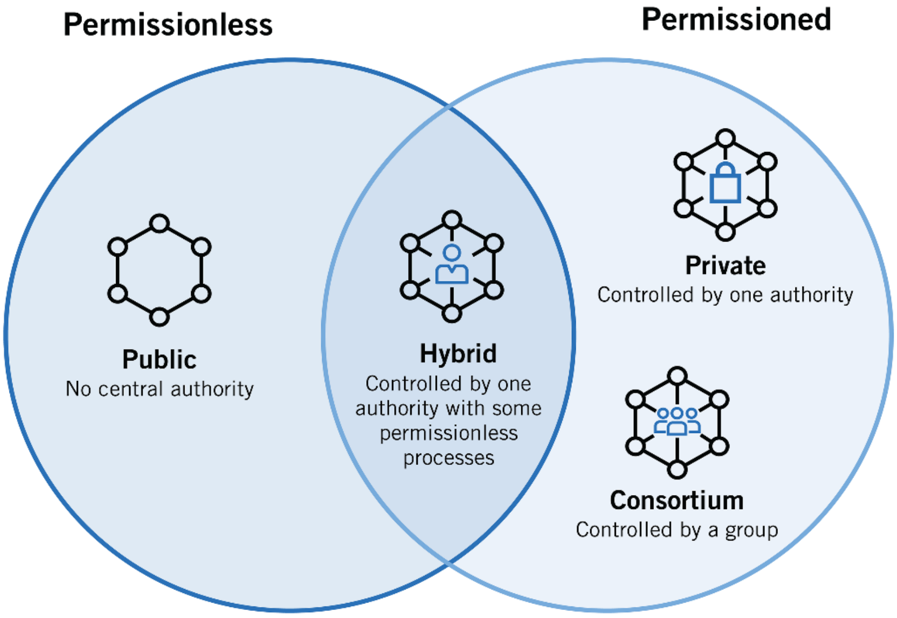


Fig 1.2: Different types of Blockchain networks

1. **Public Blockchain Network**

The public Blockchain is one that anyone can use. Also known as permissionless Blockchains. Bitcoin and Ethereum are both examples of public Blockchains. Anyone in the network can access the chain and add blocks. It may require considerable computational power, provide little or no privacy for transactions, and provide weak security.

2. **Private Blockchain Network**

Similarly, to a public Blockchain network, a private Blockchain network is also decentralized and peer-to-peer. A single organization governs the network, deciding who can participate, executing a consensus protocol and maintaining a shared ledger. Private Blockchains can be hosted privately on premise and run behind a corporate firewall.

3. **Permissioned Blockchain Networks**

Businesses who set up a private Blockchain will generally set up a permissioned Blockchain network. Furthermore, public Blockchain networks can be permissioned as well. They restrict who is permitted to participate in the network and in what transactions. It is necessary for participants to obtain an invitation or permission to join.

4. **Consortium Blockchains**

Maintaining a Blockchain can be shared by multiple organizations. A pre-selected group of organizations determines who may submit transactions or access data. When all participants need to be permissioned and be responsible for the Blockchain, a consortium Blockchain is the ideal solution.

1.10 Components of Blockchain EcoSystem

There are four main components of any Blockchain EcoSystem:

- A node application
- A shared ledger
- A consensus algorithm
- A virtual machine

A node application: In order to participate in an ecosystem, all inter connected computers that are connected to the Internet must install and run a computer application specific to that ecosystem. As an example, if we use bitcoin as an ecosystem, each computer must run the bitcoin wallet application.

A shared ledger: It is a type of data structure managed inside node application. When we launch the node application for that ecosystem, you can view its ledger (or Blockchain) contents. The interaction is based on the ecosystem in which it exists. You will have only one shared ledger for each ecosystem regardless of how many ecosystems you participate in.

A consensus Algorithm: The consensus algorithm defines how all peers in a Blockchain network agree on the current state of the distributed ledger. There are different consensuses for achieving consensus in different ecosystems based on the features they want. There are number of schemes of consensuses: proof-of-work, proof-of-stake, proof-of-elapsed-time etc., each having different characteristics.

A virtual machine: By definition, a virtual machine is a representation of a real or imaginary machine created by a computer program and provided with instructions expressed in a language**.** It is an abstraction of a machine, held inside a machine.

1.11 Core Components of Blockchain

Following are the 6 core components of Blockchain that forms the complete structure of Blockchain along with people involve in mining and rules those define mining processes:

- **Miners:** Nodes that perform verification of block
- **Consensus:** The rules and arrangements governing Blockchain operations
- **Block:** It keeps a record of transactions distributed among all members of the network
- **Node:** In the Blockchain architecture, it could be a user or a computer, each storing copy of ledger
- **Transaction:** A transfer of information from one node to another
- **Chain:** a sequence of blocks in a specific order

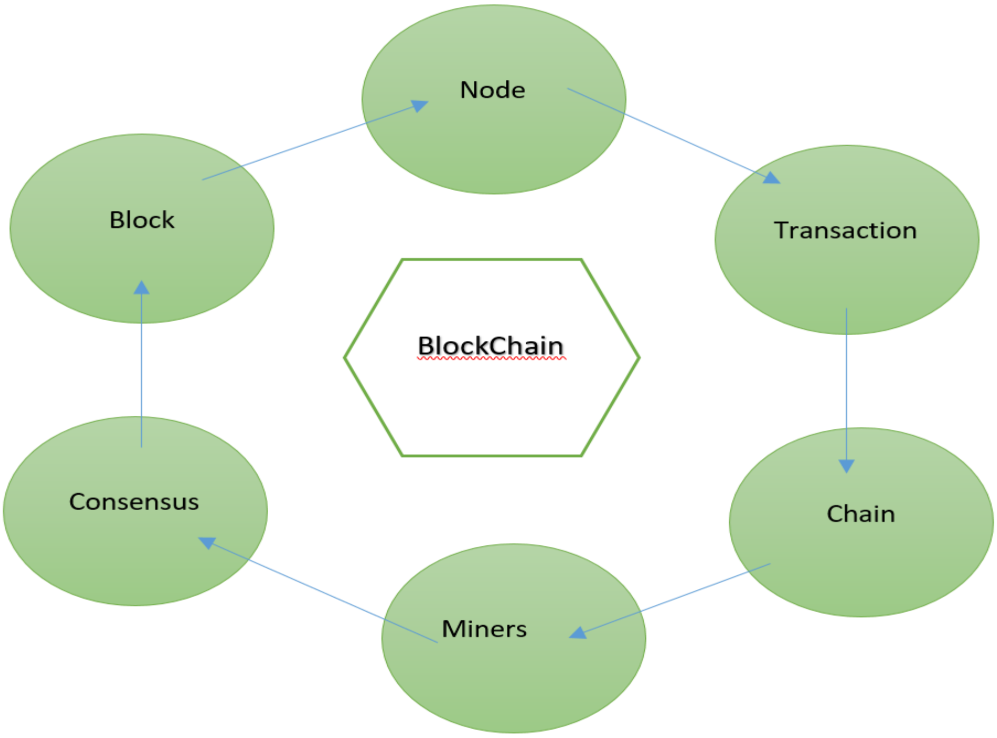


Fig 1.3: Core components of Blockchain

CHAPTER 2

LITERATURE REVIEW

2.1 Study of Various Research Papers

A literature review covers published material in a certain topic area, as well as information published within a specific time period

It is the purpose of a literature review to synthesize and summarize existing knowledge in a field without adding any new knowledge. Based on existing knowledge, they help the researcher even turn the wheels of the topic of study. Overcoming existing findings requires in-depth understanding of what is wrong with them**.**

Following are some research papers along with the discussed topics behind them:

- **Blockcahin 1.0 to Blockchain 4.0- The Evolutionary Transformation of Blockchain Technology(https://www.researchgate.net/publication/351263701; Pratyusa Mukherjee, Pratyusa Mukherjee):** They have discussed about Blockchain evolution in their paper. Blockchain is a technology that has gained enormous popularity and traction. It is a distributed ledger where each record or block is secured and bound to the succeeding blocks through hash functions, resulting in a chain of blocks. The first section of paper gives the historical background of this expeditious technology. The second section describes the basics of Blockchain, its types, a block's structure, and different consensus models.. The prime emphasis of the paper is to bestow an extensive study of the chronological evolutions in Blockchain Technology by highlighting the nitty-gritty of each generation in detail. It also illustrates a parameter wise differences amidst the several generations in terms of their principle areas, consensus models used, utility of smart contracts, the energy and cost requirements and execution speed and scalability. In the end, a Blockchain in Supply Chain Management test case has also been elaborated in this chapter.

- **A Deep Investigation on Blockchain Network based on Platforms and Consensus Algorithms (International Journal of Advanced Science and Technology Vol. 29, No. 8s, (2020), pp. 3614-3629):** Technological advances have led to an increase in data generated by various segments of the economy, including health care, banking, supply chain, agriculture, education, etc**.** Due to data breaches and privacy concerns, most industries are implementing distributed decentralized systems. The Blockchain technology is an emerging technology that helps to build analogue systems without a central facilitator or party. This paper presents a comprehensive and comparative study of the Blockchain. It explores and compares several types of Blockchain networks. Subsequently, various available Platform to develop the distributed and decentralized protocols are discussed, which are used to provide secure and transparent Internet services. At last, a comparative analysis among available consensus mechanisms is performed.

- **A Relative Study of Blockchain Mining (Imperial Journal of Interdisciplinary Research (IJIR) · May 2017):** This paper is a study on Bitcoin Mining process. Bitcoin mining is the method of adding transaction records to Bitcoin's community ledger of earlier period transactions or Blockchain. The mining practice is used to confirm and secure transactions. This method is organized as a speed game among persons or firms – the miners – with diverse computational powers to solve a mathematical difficulty, bring a proof of work, extend their solution and attain agreement among the Bitcoin network nodes with it.

- **A Novel Comparison Of Consensus Algorithms In Blockchain (Advances and Applications in Mathematical Sciences Volume 20, Issue 1, November 2020): By using consensus algorithms, secure transactions can be carried out in a distributed system which has peer-to-peer connections of blocks, without the need for a middleman**. For Blockchain technology, consensus algorithms play a crucial role in maintaining the security and integrity of distributed networks. Basically, it maintains trust in Blockchain technology. The consensus algorithms are divided into two types, proof based and voting based. The paper provides an overview of the most common 2 types of consensus algorithms that can be applied to Blockchains, and examines their strengths, weaknesses, and the types of Blockchains where these algorithms could be used.

- **Implementation of Blockchain Consensus Algorithm on Embedded Architecture (Hindawi Security and Communication Networks Volume 2021, Article ID 9918697):** In this paper, the HW implementation of the PoW consensus is depicted. This consensus is used in the Ethereum Blockchain. We were able to demonstrate that, to successfully implement this consensus on low-resource platforms, it is possible to use an on-chain system to successfully transfer and receive data and an off-chain system to implement the consensus and send the result to the on-chain node. This system, despite its complexity, allows a gain of at least 5 times compared to a pure SW system in execution time, while minimizing energy consumption. It can also be improved and accelerated by playing on the different blocks of the consensus. Indeed, we have added 4 IPs of nonce generators, but we could improve the result even more by adding more Keccak 256 and or 512 IPs to have a more efficient and faster system.

- **A Brief Analysis of Blockchain Algorithms and Its Challenges (https://www.researchgate.net/publication/348127582):** Blockchain 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 decentralized ledger and distributed database without the need for central authority verification. The paper discusses different consensus algorithms, Blockchain challenges, and their applications. 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). A discussion of the basis of Blockchain is provided, there are some mining techniques, consensus problems, and comparison algorithms according to performance.

- **Blockchain Consensus Algorithms: A Survey (https://www.researchgate.net/publication/338738073):** The sky-rocket anticipation of Blockchain potential has caused a wide-scale exploration of its usage in different application domains. As a result, there are a variety of Blockchain systems available. Although Blockchains promise to revolutionize the way we store and transmit data, they suffer from serious performance and security shortcomings, which will need to be addressed before wide-scale adoption can take place. A Blockchain system's underlying consensus algorithm is crucial for its performance and security, since it determines the system's overall performance. Therefore, to address the limitations of different Blockchain systems, several existing as well novel consensus algorithms have been introduced. By systematically examining these algorithms, we can figure out how and why any particular Blockchain functions as it does.

- **Comparisons of Blockchain based Consensus Algorithms for Security Aspects (International Journal on Emerging Technologies 11(3)):** Blockchain’s first implementation attention is crypto-currency. In this new distributed architecture, which is decentralized and has no central authority, Blockchain serves as an immutable distributed ledger for processing transactions with the participation of untrusted parties. Smart contracts allow states to be shared and transactions to be executed by participants in this decentralized network. Blockchain applications are crypto-currency based online wallets, Internet of Things, springing up, financial services, risk management, reputation system, etc. This paper aims to share knowledge on the growing importance of Blockchain technology in real-world applications. Furthermore, this paper provides a comparison of typical consensus algorithms for security aspects as part of Blockchain core components and technologies. According to this comparison and Blockchain applications, alternative Merkel tree based Blockchains are available in the market for faster and more secure transactions.

- **A Survey about Consensus Algorithms Used in Blockchain (Journal of Information Processing System): The key contribution of Blockchain lies in its consensus algorithm, which determines how agreements are made among all nodes in the verifying network to append a new block**. Blockchain algorithms can be categorized into two main groups. The first group is proof-based consensus, in order to be included in the verifying network, nodes must qualify themselves as more qualified than their peers. The second group is voting-based consensus, to verify a new block or transaction, each node in the network must share their results before making a final decision. This paper provides a review of some Blockchain consensus algorithms that have been researched and that are currently being applied to some well-known applications.

- **Survey of Blockchain Consensus Algorithms (EasyChair Preprint):** A testament to the rapid transition of world order from the centralised means of operation to progressive decentralisation is the growing popularity of the Blockchain technology. Much of this can be accredited to its revolutionising principles of maintaining irreversible, tamper-free and distributed records. However, despite welcoming this technology with open arms most companies are still struggling to replace their conventional models with Blockchain. This problem is spawned by the lack of exhaustive research that draws boundaries between the vast amount of consensus algorithms that developers are flooded with. To cater to the dire need of laying benchmarks for consensus algorithms, this paper attempts to list down comprehensive parameters that organisations could refer to in order to adopt the Blockchain model effectively. It further does an exhaustive comparison of popular consensus protocols against these parameters.

- **A Research Survey on Applications of Consensus Protocols in Blockchain (Hindawi Security and Communication Networks Volume 2021, Article ID 6693731):** The concept of Blockchain, widely known as virtual currencies, saw a massive surge in popularity in recent times. As far as the security of the Blockchain is concerned, consensus algorithms play a vital role in the Blockchain. Research has been done separately, or comparisons between a few of them have been presented previously. In this paper, we have discussed widely used consensus algorithms in the Blockchain. +e consensus protocols covered in this paper include PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), PoET (Proof of Elapsed Time), PBFT (Practical Byzantine Fault Tolerance), and PoA (Proof of Authority). For each consensus, we have reviewed the properties, applications, and performance in the Blockchain

- **A Survey of Consensus Algorithms for Blockchain Technology (Imam Abdulrahman Bin Faisal Univarsity P.O.Box 1982, Dammam 31441, Saudi Arabia):** Blockchain technology is a new shift in the Internet world, it has brought about changes in many sectors. Where transactions can be securely accomplished via point-topoint connections in a distributed system without the need for a third-party, with the help of consensus algorithms. In this paper, we will conduct a comprehensive survey on the Blockchain technology with focusing in the popular consensus algorithms, in order to figure out their features, and the factors that affect the performance and security. Also, we will provide a classification of the consensus algorithms and we will perform a comprehensive comparison of studied consensus algorithms. In addition, we will provide a detailed discussion of the consensus algorithms that studied with an analysis of the main factors affecting these algorithms. Finally, we will refer to some recommendations that must be considered and which can contribute to the development of this area.

- **Consensus Algorithms in Blockchain Technology: A Survey (IEEE – 45670):** Blockchain is an immutable, transparent, public ledger that is distributed among the nodes in the network. It is a decentralized system in which transactions run on untrusted devices. To ensure equality and fairness, these transactions need to agree on some protocols. They are known as consensus algorithms. They are the core of Blockchain and decide how Blockchain works. Applying these algorithms, it is almost impossible for unauthorized users to crack the confidential information in the blocks. However, there are some security and performance issues that are required to be improved. In this paper, we have an overlook on various consensus algorithms, their working and where they are applied. In addition, we have reviewed Blockchain technology, its application areas, advantages, and issues.

- **A review on consensus algorithm of Blockchain (2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)):** Blockchain is the basic technology of bitcoin. With the value appreciation and stable operation of bitcoin, Blockchain is attracting more and more attention in many areas. Blockchain has the characteristics of decentralization, stability, security, and non-modifiability. It has the potential to change the network architecture. The consensus algorithm plays a crucial role in maintaining the safety and efficiency of Blockchain. Using a right algorithm may bring a significant increase to the performance of Blockchain application. In this paper, we reviewed the basic principles and characteristics of the consensus algorithms and analyzed the performance and application scenarios of different consensus mechanisms. We also gave a technical guidance of selecting a suitable consensus algorithm and summarized the limitations and future development of Blockchain technology.

- **Comparative analysis of Blockchain consensus algorithms(IEEE, 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)):** Cryptocurrencies have seen a massive surge in popularity and behind these new virtual currencies is an innovative technology called the Blockchain: a distributed digital ledger in which cryptocurrency transactions are recorded after having been verified. The transactions within a ledger are verified by multiple clients or “validators,” within the cryptocurrency's peer-to-peer network using one of many varied consensus algorithms for resolving the problem of reliability in a network involving multiple unreliable nodes. The most widely used consensus algorithms are the Proof of Work (PoW) algorithm and the Proof of Stake (PoS) algorithm; however, there are also other consensus algorithms which utilize alternative implementations of PoW and PoS, as well as other hybrid implementations and some altogether new consensus strategies. In this paper, we perform a comparative analysis of typical consensus algorithms and some of their contemporaries that are currently in use in modern Blockchains. Our analysis focuses on the algorithmic steps taken by each consensus algorithm, the scalability of the algorithm, the method the algorithm rewards validators for their time spent verifying blocks, and the security risks present within the algorithm. Finally, we present our conclusion and some possible future trends for consensus algorithms used in Blockchains.

- **A survey of Blockchain consensus algorithms performance evaluation criteria (Expert Systems with Applications Volume 154, 15 September 2020, 113385):** How to reach an agreement in a Blockchain network is a complex and important task that is defined as a consensus problem and has wide applications in reality including distributed computing, load balancing, and transaction validation in Blockchains. Over recent years, many studies have been done to cope with this problem. In this paper, a comparative and analytical review on the state-of-the-art Blockchain consensus algorithms is presented to enlighten the strengths and constraints of each algorithm. Based on their inherent specifications, each algorithm has a different domain of applicability that yields to propose several performance criteria for the evaluation of these algorithms. To overview and provide a basis of comparison for further work in the field, a set of incommensurable and conflicting performance evaluation criteria is identified and weighted by the pairwise comparison method. These criteria are classified into four categories including algorithms’ throughput, the profitability of mining, degree of decentralization and consensus algorithms vulnerabilities and security issues. Based on the proposed framework, the pros and cons of consensus algorithms are systematically analyzed and compared in order to provide a deep understanding of the existing research challenges and clarify the future study directions.

- **Survey on Private Blockchain Consensus Algorithms (2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)):** A Blockchain is a distributed ledger of records called as blocks. These blocks are linked using cryptographic hash. Each block contains a hash of the previous block, a timestamp, and transaction data. Consensus layer is the main layer in Blockchain Architecture, in which consensus protocol is configured to decide how new block is added in Blockchain. Consensus algorithm solves the problem of trust in Blockchain. Consensus algorithms can be classified into two classes. The first class is voting-based consensus, which requires nodes in the Blockchain network to broadcast their results of mining a new block or transaction, before appending the block to Blockchain. The second class is proof-based consensus, which requires the nodes joining the Blockchain network to solve and mathematical puzzle to show that they are more eligible than the others to do the appending or mining work. Performance of Blockchain can be increased with the use of suitable consensus algorithm. However, theory and data support for the selecting suitable consensus in private Blockchain is very limited. This paper contributes theory and data used for selecting suitable consensus algorithm and would help researchers for further exploring of consensus in private Blockchain environment.

- **Blockchain Consensus Algorithms: A Survey:** In recent years, Blockchain technology has received unparalleled attention from academia, industry, and governments all around the world. It is considered a technological breakthrough anticipated to disrupt several application domains. This has resulted in a plethora of Blockchain systems for various purposes. However, many of these Blockchain systems suffer from serious shortcomings related to their performance and security, which need to be addressed before any wide-scale adoption can be achieved. A crucial component of any Blockchain system is its underlying consensus algorithm, which in many ways, determines its performance and security. Therefore, to address the limitations of different Blockchain systems, several existing as well novel consensus algorithms have been introduced. A systematic analysis of these algorithms will help to understand how and why any particular Blockchain performs the way it functions. However, the existing studies of consensus algorithms are not comprehensive. Those studies have incomplete discussions on the properties of the algorithms and fail to analyse several major Blockchain consensus algorithms in terms of their scopes. The result of the analysis is presented in tabular formats, which provides a visual illustration of these algorithms in a meaningful way. We have also analysed more than hundred top crypto-currencies belonging to different categories of consensus algorithms to understand their properties and to implicate different trends in these crypto-currencies. Finally, they have presented a decision tree of algorithms to be used as a tool to test the suitability of consensus algorithms under different criteria.

- **A Survey about Consensus Algorithms Used in Blockchain (Journal of Information Processing Systems):** Blockchain has recently been nominated as one of the technologies exciting intense attention. Blockchain has solved the problem of changing the original low-trust centralized ledger held by a single third-party, to a high-trust decentralized form held by different entities, or in other words, verifying nodes. The key contribution of the work of Blockchain is the consensus algorithm, which decides how agreement is made to append a new block between all nodes in the verifying network. Blockchain algorithms can be categorized into two main groups. The first group is proof-based consensus, which requires the nodes joining the verifying network to show that they are more qualified than the others to do the appending work. The second group is voting-based consensus, which requires nodes in the network to exchange their results of verifying a new block or transaction, before making the final decision. In this paper, we present a review of the Blockchain consensus algorithms that have been researched and that are being applied in some well-known applications at this time.

- **From Blockchain consensus back to Byzantine consensus (Future Generation Computer Systems):** In this paper, they have discussed the mainstream Blockchain consensus algorithms and how the classic Byzantine consensus can be revisited for the Blockchain context. In particular, we discuss proof-of-work consensus and illustrate the differences between the Bitcoin and the Ethereum proof-of-work consensus algorithms. Based on these definitions, we warn about the dangers of using these Blockchains without understanding precisely the guarantees their consensus algorithm offers. In particular, we survey attacks against the Bitcoin and the Ethereum consensus algorithms. We finally discuss the advantage of the recent Blockchain Byzantine consensus definition over previous definitions, and the promises offered by emerging consistent Blockchains.

- **A survey of Blockchain consensus algorithms: mechanism, design and applications:** In 2008, Blockchain was introduced to the world as the underlying technology of the Bitcoin system. After more than a decade of development, various Blockchain systems have been proposed by both academia and industry. This paper focuses on the consensus algorithm, which is one of the core technologies of Blockchain. In this paper, we propose a unified consensus algorithm process model that is suitable for Blockchains based on both the chain and directed acyclic graph (DAG) structure. Subsequently, we analyze various mainstream Blockchain consensus algorithms and classify them according to their design in different phases of the process model. Additionally, we present an evaluation framework of Blockchain consensus algorithms and then discuss the security design principles that enable resistance from different attacks. Finally, we provide some suggestions for selecting consensus algorithms in different Blockchain application scenarios.

- **Research on Progress of Blockchain Consensus Algorithm:** A Review on Recent Progress of Blockchain Consensus Algorithms: Blockchain technology can solve the problem of trust in the open network in a decentralized way. It has broad application prospects and has attracted extensive attention from academia and industry. The Blockchain consensus algorithm ensures that the nodes in the chain reach consensus in the complex network environment, and the node status ultimately remains the same. The consensus algorithm is one of the core technologies of Blockchain and plays a pivotal role in the research of Blockchain technology. This article gives the basic concepts of the Blockchain, summarizes the key technologies of the Blockchain, especially focuses on the research of the Blockchain consensus algorithm, expounds the general principles of the consensus process, and classifies the mainstream consensus algorithms. Then, focusing on the improvement of consensus algorithm performance, it reviews the research progress of consensus algorithms in detail, analyzes and compares the characteristics, suitable scenarios, and possible shortcomings of different consensus algorithms, and based on this, studies the future development trend of consensus algorithms for reference.

- **Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism:** Blockchain technology has a wide range of applications in the fields of finance, credit reporting and intellectual property, etc. As the core of Blockchain, consensus algorithm affects the security and performance of Blockchain system directly. In the past 10 years, there have been about 30 consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Ripple Protocol Consensus Algorithm (RPCA) and AlgoRand. But their security, stability and operating efficiency still lag far behind our actual needs.

  This paper introduces the computing power competition of PoW into DPoS to design an improved consensus algorithm named Delegated Proof of Stake with Downgrade (DDPoS). Through the further modification, the impact of both computing resources and stakes on generating blocks is reduced to achieve higher efficiency, fairness, and decentralization in consensus process. Then a downgrade mechanism is proposed to quickly replace the malicious nodes to improve the security. The simulation experiments in Blockchain system show that the proposed consensus algorithm is significantly more efficient than PoW and PoS, but slightly lower than DPoS. However, its degree of centralization remains far below that of DPoS. And through the downgrade mechanism, the proposed consensus algorithm can detect and downgrade the malicious nodes timely to ensure the security and good operation of system.

CHAPTER 3

CONSENSUS ALGORITHMS

3.1 OVERVIEW

In simple terms, Blockchain consensus algorithm is a process through which peers of a Blockchain network determine the real-time state of a distributed ledger by reaching a consensus. In Blockchain networks, consensus mechanisms assist nodes in achieving reliability and building trust between each other, while ensuring environmental security. For this reason, it is a key component of every Blockchain app development guide and every distributed ledger app project**.**

Through a consensus algorithm, all parties to the Blockchain network agree (consensus) on the data state of the ledger and can trust unknown peers in the distributed computing environment.

3.2 Objectives of consensus algorithms

Following are the objectives of Consensus Algorithms:

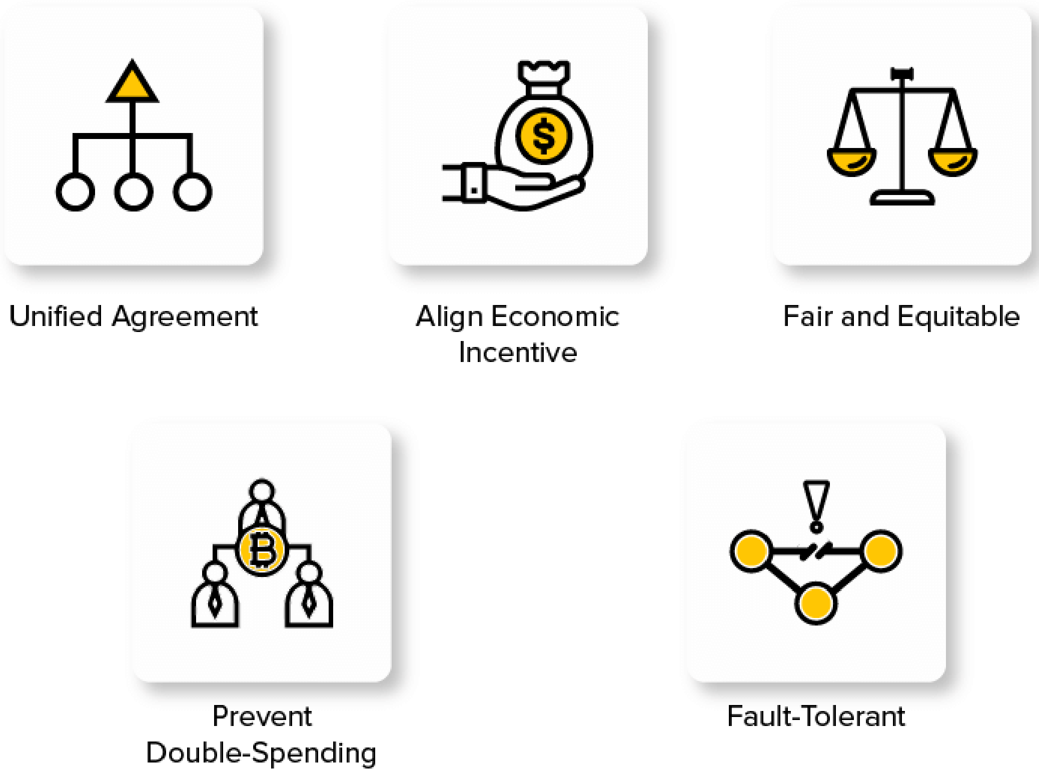


Fig 3.1: Objectives of Consensus Algorithms of Blockchain

1. **Fault Tolerance and Economic Security**

A consensus algorithm's security relates to its fault tolerance. Blockchain security is actually a composite of many different properties but that's an article for another day. The ability of a system to tolerate some malfunctioning of its components is called fault tolerance. System malfunctions can be caused by a variety of faults including software or hardware bugs such as stack overflows or fatigued components.

The governed system would work indefinite times even in the case of failures and threats.

2. **Unified Agreement**

Attaining unified agreement is one of the primary objectives of consensus mechanisms. Decentralized systems, in contrast to centralized systems, permit users to operate without trusting authority. As a result of the protocols embedded in the Distributed Blockchain network, the data involved in the process is true and accurate, and the public ledger is updated regularly.

3. Align Economic Incentive

The interests of participants in the network must be aligned when creating a trustless system that regulates itself.
Consensus Blockchain protocols reward good behavior and punish bad behavior in this situation. This way, it ensures regulating economic incentives too.

4. Fair & Equitable

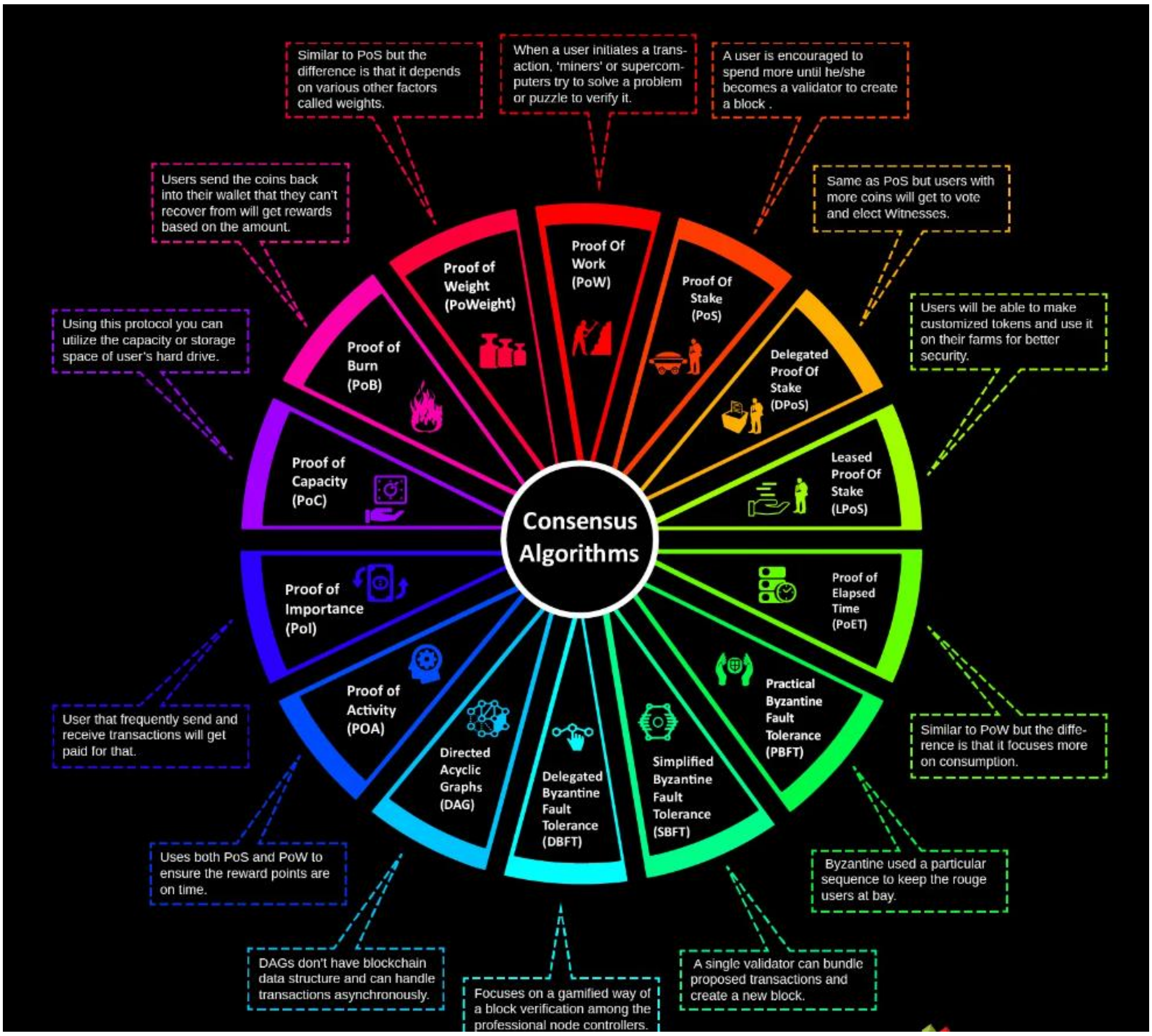
Consensus mechanisms allow any individual to participate in the network and use the same basics. Therefore, it justifies the decentralization and open-source properties of the Blockchain technology.

5. Prevent Double Spending

Based on certain algorithms, consensus mechanisms ensure that only verified and legitimate transactions are published in the public ledger. This solves the traditional problem of double-spending, i.e, the problem of spending a digital currency twice.

3.3 Types of Consensus Algorithms

For Blockchain networks, the consensus algorithms are an essential element because they maintain the integrity and security of these distributed computing systems. Below are the different types of Blockchain consensus systems that are popular today:


Consensus Algorithms
Proof Of Work (PoW)
Proof Of Stake (PoS)
Delegated Proof Of Stake (DPoS)
Leased Proof Of Stake (LPoS)
Proof of Elapsed Time (PoET)
Practical Byzantine Fault Tolerance (PBFT)
Simplified Byzantine Fault Tolerance (SBFT)
Delegated Byzantine Fault Tolerance (DBFT)
Directed Acyclic Graphs (DAG)
Proof of Activity (POA)
Proof of Importance (PoI)
Proof of Capacity (PoC)
Proof of Burn (PoB)
Proof of Weight (PoWeight)

When a user initiates a transaction, 'miners' or supercomputers try to solve a problem or puzzle to verify it.

A user is encouraged to spend more until he/she becomes a validator to create a block .

Same as PoS but users with more coins will get to vote and elect Witnesses.

Users will be able to make customized tokens and use it on their farms for better security.

Similar to PoW but the difference is that it focuses more on consumption.

Byzantine used a particular sequence to keep the rouge users at bay.

A single validator can bundle proposed transactions and create a new block.

Focuses on a gamified way of a block verification among the professional node controllers.

DAGs don't have blockchain data structure and can handle transactions asynchronously.

Uses both PoS and PoW to ensure the reward points are on time.

User that frequently send and receive transactions will get paid for that.

Using this protocol you can utilize the capacity or storage space of user's hard drive.

Users send the coins back into their wallet that they can't recover from will get rewards based on the amount.

Similar to PoS but the difference is that it depends on various other factors called weights.

Fig 3.2: A brief overview of each Consensus Algorithm

3.3.1 Proof of Work (PoW)

Developed by Satoshi Nakamoto, Proof of Work is the oldest consensus mechanism used in the Blockchain domain. It is also known as mining where the participating nodes are called miners. In this mechanism, the miners have to solve complex mathematical puzzles using comprehensive computation power. They use different forms of mining methods, such as GPU mining, CPU mining, ASIC mining, and FPGA mining. And the one that solves the problem at the earliest gets a block as a reward.

The Proof of Work mechanism is used by multiple cryptocurrencies like Bitcoin, Litecoin, ZCash, Primecoin, Monero, and Vertcoin etc. In bitcoin consensus algorithm each block is intended to generate a hash value, and the nonce is the parameter that is used to generate that hash value. The Proof of Work (PoW) has not only influenced the financial industry, but also healthcare, governance, management and more. It has, in fact, offered the opportunity of multichannel payments and multi-signature transactions over an address for enhancing security.

3.3.2 Proof of Stake (PoS)

The most basic and environmentally-friendly alternative of PoW consensus protocol.The block producers are not miners, but they act like validators. They get the opportunity to create a block over everyone which saves energy and reduces the time. However, for them to become a validator, they are supposed to invest some amount of money or stake. Also, unlike that in the case of PoW, miners are provided with a privilege to take their transaction fees in this algorithm for there is no reward system in this consensus model.

This, as a whole, encouraged brands like Ethereum to upgrade their model from PoW to PoS in their Ethereum 2.0 update. Also, it helped various Blockchain ecosystems like Dash, Peercoin, Decred, Reddcoin, and PivX to function properly. Now, while PoS solved various issues earlier associated with PoW, there were many challenges still undusted in the market. To mitigate those challenges and deliver an enhanced Blockchain environment, several variations of PoS came into existence.

The two popular variations of Proof of Stake (PoS) are DPoS and LPoS.

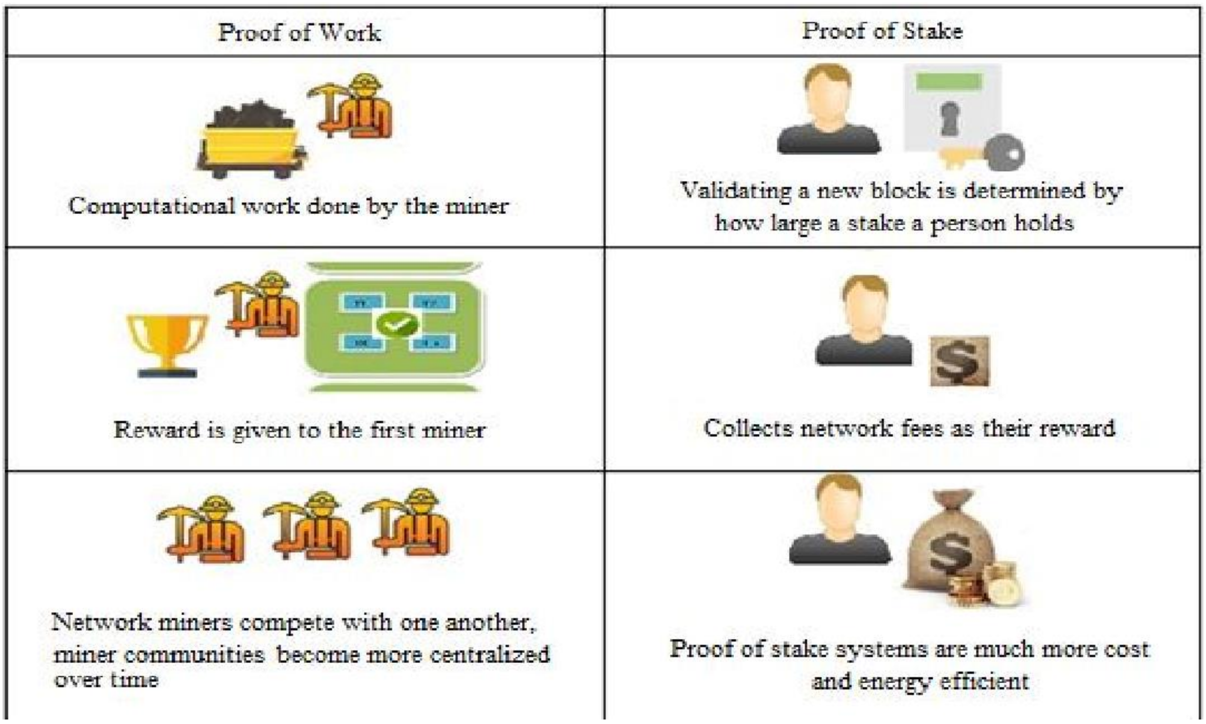
1. Delegated Proof of Stake (DPoS)

In the case of Delegated Proof of Stake (DPoS), the participants stake their coin and vote for a certain number of delegates such that the more they invest, the more weightage they receive. For example: if user A spends 10 coins for a delegate and user B invests 5 coins, A’s vote gets more weightage than that of B. The delegates also get rewarded in the form of transaction fees or a certain amount of coins. Because of this stake-weighted voting mechanism, DPoS is one of the fastest Blockchain consensus models and highly preferred as a digital democracy. Some of the real-life use cases of this Blockchain consensus mechanism are Steem, EOS, and BitShares.

2. Leased Proof of Stake (LPoS)

LPoS is an enhanced version of PoS consensus mechanism that operates on the Waves platform.

Unlike the regular Proof-of-Stake method where each node with some amount of cryptocurrency is entitled to add the next Blockchain, users can lease their balance to full nodes in this consensus algorithm Blockchain. And the one that leases the bigger amount to the full node has a higher probability of generating the next block. Also, the leaser is then rewarded with a percentage of transaction fee that has been collected by the complete node. This PoS variant is an efficient and safe option for the development of public cryptocurrencies.



Proof of Work	Proof of Stake
Computational work done by the miner	Validating a new block is determined by how large a stake a person holds
Reward is given to the first miner	Collects network fees as their reward
Network miners compete with one another, miner communities become more centralized over time	Proof of stake systems are much more cost and energy efficient

Fig 3.3: Differences between PoW and PoS

3.3.3 Proof of Authority (PoAu)

Proof of Authority is a modified version of Proof of Stake in which the identities of validators in the network are at stake. In this, to verify the validator’s identity, the identity is the resemblance between validators’ personal identification and their official documentation. These validators put their reputation on the network. In Proof of Authority, the nodes (that become validators) are the only ones allowed to produce new blocks. Validators whose identity is at risk are incentivized to secure and preserve the Blockchain network. In this proof, the number of validators are fairly small, around 25 or less.

3.3.4 Byzantine Fault Tolerance (BFT)

Byzantine Fault Tolerance, as the name suggests, is used to deal with Byzantine fault (also called Byzantine Generals Problem) – a situation where the system’s actors have to agree on an effective strategy so as to circumvent catastrophic failure of the system, but some of them are dubious.

Two Variations of BFT are:

3.3.4.1 Practical Byzantine Fault Tolerance (PBFT)

PBFT is a lightweight Blockchain algorithm that solves the Byzantine General’s problems by letting users confirm the messages that have been delivered to them by performing a computation to evaluate the decision about the message’s validity. The party then announces its decision to other nodes who ultimately process a decision over it. This way, the final decision relies upon the decisions retrieved from the other nodes. Stellar, Ripple, and Hyperledger Fabric are some use cases of this Blockchain consensus mechanism.

3.3.4.2 Delegated Byzantine Fault Tolerance (DBFT)

Introduced by NEO, the Delegated Byzantine Fault Tolerance mechanism is similar to the Delegated Proof of Stake (DPoS) consensus model. Here also, the NEO token holders get the opportunity to vote for the delegates. However, this is independent of the amount of currency they invest. Anyone who fulfills the basic requirements, i.e., a verified identity, right equipment, and 1,000 GAS, can become a delegate. One among those delegates is then chosen as speaker randomly**.** The speaker creates a new block from the transaction that is waiting to be validated. Also, he sends a proposal to the voted delegates who have the responsibility to supervise all the transactions and record them on the network. These delegates have the freedom to share and analyze the proposals to check the accuracy of data and honesty of the speaker. If then, 2/3rd of the delegates validates it, the block is added to the Blockchain.

This type of Blockchain consensus protocol is also called ‘Ethereum of China’ and can be a helpful resource in building a ‘smart economy’ by digitizing assets and offering smart contracts on the Blockchain.

3.3.5 Direct Acyclic Graph (DAG)

In this type of Blockchain consensus protocol, every node itself prepares to become the ‘miners’. Now, when miners are eradicated and transactions are validated by users itself, the associated fee reduces to zero. It becomes easier to validate transactions between any two closest nodes, which makes the whole process lightweight, faster, and secure. The two best examples of DAG algorithms are IOTA and Hedera Hashgraph.

3.3.6 Proof of Capacity (PoC)

In the Proof of Capacity (PoC) mechanism, solutions for every complex mathematical puzzle are accumulated in digital storages like Hard disks. Users can use these hard disks to produce blocks, in a way that those who are fastest in evaluating the solutions get better chances for creating blocks. The process it follows is called Plotting. The two cryptocurrencies that rely on PoC Blockchain consensus protocol are Burstcoin and SpaceMint.

3.3.7 Proof of Burn (PoB)

This is alternate solution to PoW and PoS in terms of energy consumption. Proof of Burn (PoB) consensus model works on the principle of letting miners ‘burn’ or ‘ruin’ the virtual cryptocurrency tokens, which further provides them with a privilege to write blocks in proportion to the coins. The more coins they burn, the more are the chances of picking the new block for every coin they get. But, in order to burn coins, they are required to send it to the address where it couldn't be spent for verifying the block. This is widely employed in the case of distributed consensus. And the finest example of this consensus mechanism is the Slim coin.

3.3.8 Proof of Identity (PoId)

The concept of PoI (Proof of Identity) is just like that of the authorized identity. It is a piece of cryptographic confirmation for a users' private key that is being attached to each particular transaction. Each identified user can create and manage a block of data that can be presented to others in the network. This Blockchain consensus model ensures authenticity and integrity of the created data. And thus, it is a good choice for introducing smart cities.

3.3.9 Proof of Activity (PoAc)

It is the convergence of PoW and PoS Blockchain consensus models. In the case of PoA mechanism, miners race to solve a cryptographic puzzle at the earliest using special hardware and electric energy, just like in PoW. However, the blocks they come across hold only the information about the identity of the block winner and reward transaction. This is where the mechanism switches to PoS. The validators (shareholders appointed to validate transactions) test and ensure the correctness of the block. If the block was checked many times, the validators activate to a complete block. This confirms that open transactions are processes and are finally integrated into the found block containers. Besides, the block reward is divided so that validators gain shares of it. E.g. Espers and Decred coins.

3.3.10 Proof of Elapsed Time (PoET)

PoET was introduced by Intel with an intent to take over cryptographic puzzles involved in PoW mechanism by considering the fact that the CPU architecture and the quantity of mining hardware knows when and at what frequency does a miner win the block. It is based on the idea of fairly distributing and expanding the odds for a bigger fraction of participants. And so, every participating node is asked to wait for a particular time to participate in the next mining process. The member with the shortest hold-up time is asked to offer a block. At the same time, every node also comes up with their own waiting time, after which they go into sleep mode. So, as soon as a node gets active and a block is available, that node is considered as the ‘lucky winner’. This node can then spread the information throughout the network, while maintaining the property of decentralization and receiving the reward.

3.3.11 Proof of Importance (PoI)

Introduced by NEM, PoI is a variation of PoS protocol that considers the role of shareholders and validators for its operation. However, this is not only influenced by the size and chance of their shares; various other factors like reputation, overall balance, and no. of transactions made through any particular address also plays a role in it. The networks based on POI consensus model are expensive to attack on and rewards users for contributing to the network’s security.

3.3.12 Proof of Space (PoS)

Proof of space (PoS) is a type of consensus algorithm achieved by demonstrating one's legitimate interest in a service (such as sending an email) by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider. The concept was formulated in 2013 by Dziembowski and (with a different formulation) by Ateniese. Proofs of space are very similar to proofs of work (PoW), except that instead of computation, storage is used to earn cryptocurrency. Proof-of-space is different from memory-hard functions in that the bottleneck is not in the number of memory access events, but in the amount of memory required.

3.3.13 Proof of Weight (PoWeight)

Proof-of-weight consensus mechanisms are based on the Algorand consensus model, developed by researchers at the MIT Computer Science & Artificial Intelligence

Laboratory. The Algorand protocol facilitates very quick transactions by relying on a Byzantine agreement protocol, which also makes it capable of scaling to many users.
In a network utilizing proof-of-weight, weighted users play an integral role in the process of achieving consensus. Every user is assigned a certain “weight”, which is relative to a selected value that represents a user’s contribution to the network. In order to prevent double-spending attacks and other foul play on the Blockchain, the majority (more than two thirds) of the weighted fraction has to belong to honest users.

3.3.14 Proof of Devotion (PoD)

Blockchain consensus algorithm that selects accounts with high influence -- (as determined by their liquidity and propagation) -- to be block validators and proposers. Proof-of-devotion (PoD) is a Blockchain consensus algorithm researched and developed by the team behind the Nebulas cryptocurrency. PoD is similar to another consensus algorithm, proof-of-importance, because both use a sort of ranking system based on set criteria to determine who is eligible to validate and propose blocks. In PoD, eligibility is determined by how high of influence an account has, where influence is based on liquidity and propagation

3.3.15 PAXOS

Paxos is a family of consensus protocols, that ensure replica consistency in a distributed system of unreliable processors (that is servers can fail). The Paxos protocol was introduced in 1989 by Leslie Lamport, named after a fictional legislative consensus system used on the Paxos island in Greece. The objective of Paxos is To maintain the same ordering of commands among multiple replicas so that all the replicas eventually converge to the same value. This is similar to the case where multiple cars following the same directions arrive at the same final destination.

3.3.16 RAFT

Raft is a distributed consensus algorithm. It was designed to be easily understood. It solves the problem of getting multiple servers to agree on a shared state even in the face of failures. The shared status is usually a data structure supported by a replicated log. We need the system to be fully operational as long as a majority of the servers are up. Raft works by electing a leader in the cluster. The leader is responsible for accepting client requests and managing the replication of the log to other servers. The data flows only in one direction: from leader to other servers.

3.3.17 Ripple

The Ripple Protocol consensus algorithm **(**RPCA**)** is a process performed every few seconds by the nodes in the network to reach a consensus in the network. The ledger will remain in the closed state after the network nodes successfully agree. The RPCA has a few mandatory steps to go through before a transaction is successfully added to the ledger:

1. Each server collects all the known valid transactions that are not already part of the ledger and makes them public. These unconfirmed transactions are called the candidate list of transactions.
2. Each server collects all the candidate lists from the UNL servers. Transactions that receive the required number of positive votes are selected for the next step.
3. Finally, it is done

3.3.18 ERC20

ERC-20 has emerged as the technical standard; it is used for all smart contracts on the Ethereum Blockchain for token implementation and provides a list of rules that all Ethereum-based tokens must follow. ERC-20 is similar, in some respects, to bitcoin, Litecoin, and any other cryptocurrency; ERC-20 tokens are Blockchain-based assets that have value and can be sent and received. The primary difference is that instead of running on their own Blockchain, ERC-20 tokens are issued on the Ethereum network.

3.3.19 ERC-721

ERC-721 is a free, open standard that describes how to build non-fungible or unique tokens on the Ethereum Blockchain. While most tokens are fungible (every token is the same as every other token), ERC-721 tokens are all unique.

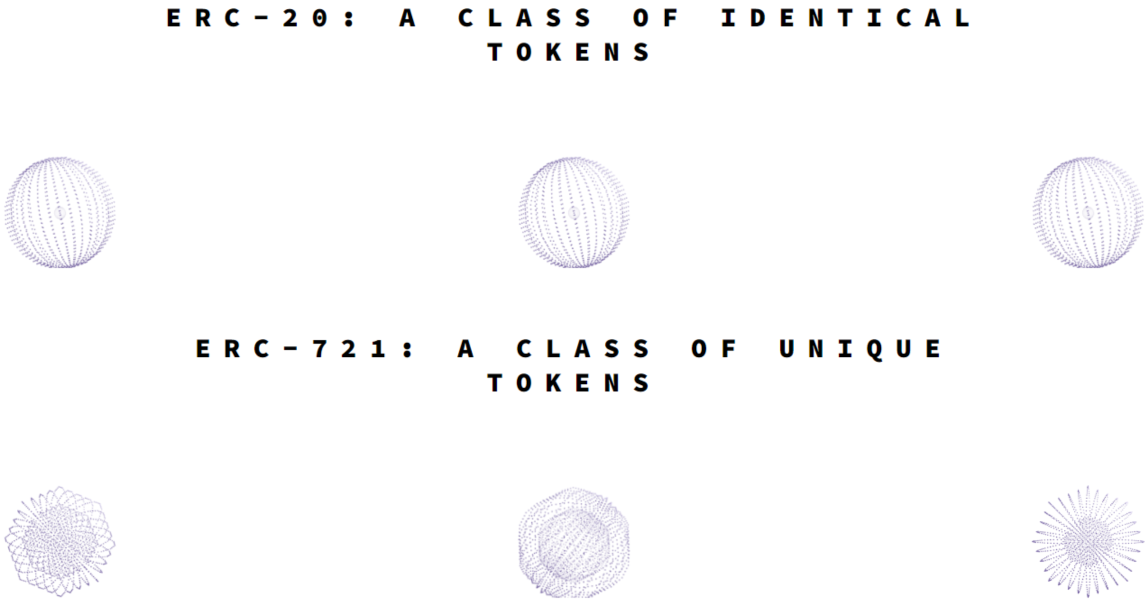

ERC-20: A CLASS OF IDENTICAL TOKENS
ERC-721: A CLASS OF UNIQUE TOKENS

Fig 3.4: Tokens of ERC-20 and ERC-721

3.3 Comparison Among The Consesns Algorithms

Below is the table for comparative study of various Consensus Algorithms on the following parameters:

4 Blockchain Platform they support

5 Year in which algorithm was launched

6. Programming Languages they support
7. Either they support Smart Contracts or not
8. Pros
9. Cons

Consensus Algorithms	Blockchain Platform	Launched Since	Programming Languages	Smart Contracts	Pros	Cons
PoW	Bitcoin	2009	C++	No	Less opportunity for 51% attack Better Security	Greater energy consumption Centralization of Miners
PoS	NXT	2013	Java	Yes	Energy efficient More decentralized	Nothing-at-stake problem
DPoS	Lisk	2016	JavaScript	No	Energy efficient Scalable Increased security	Partially centralized Double spend attack
LPoS	Waves	2016	Scala	Yes	Fair usage Lease Coins	Decentralization Issue
PoET	Hyperledger Sawtooth	2018	Python, JavaScript, Go, C++, Java, and Rust	Yes	Cheap participation	Need for specialized hardware Not good for Public Blockchain
PBFT	Hyperledger Fabric	2015	JavaScript, Python, Java REST and Go	Yes	No Need for Confirmation Reduction in Energy	Communication Gap Sybil Attack
SBFT	Chain	2014	Java, Node, and Ruby	No	Good Security Signature Validation	Not for Public Blockchain

DBFT	NEO	2016	Python,.NET, Java, C++, C, Go, Kotlin, JavaScript	Yes	Scalable Fast	Conflictions in the Chain
DAG	IOTA	2015	Javascript, Rust, Java Go, and C++	In Process	Low cost network Scalability	Implementation gaps Not suited for smart contracts
POA	Decred	2016	Go	Yes	Reduces the probability of the 51% attack Equal contribution	Greater energy consumption Double signing
PoI	NEM	2015	Java, C++XEM	Yes	Vesting Transaction partnership	Decentralization Issue
PoC	Burstcoin	2014	Java	Yes	Cheap Efficient Distributed	Favoring bigger fishes Decentralization issue
PoB	Slimcoin	2014	Python, C++, Shell, JavaScript	No	Preservation of the network	Not for short term investors Wasting coins
PoWeight	Filecoin	2017	SNARK/STARK	Yes	Scalable Customizable	Issue with Incentivization

Table 3.1: Table shows comparison among various Consensus Algorithms

CHAPTER 4

SMART CONTRACTS

4.1 What are Smart Contracts

Smart contracts are self-executing contracts in which the contents of the buyer-seller agreement are inscribed directly into lines of code. According to Nick Szabo, an American computer scientist who devised a virtual currency called "Bit Gold" in 1998, Smart contracts are computerized transaction protocols that execute contract conditions. Using it makes the transactions traceable, transparent, and irreversible. Typically, they automate the execution of agreements so that all parties can be sure of the outcome without the involvement of intermediaries or time loss.

Smart contracts are self-executing lines of code with the terms of an agreement between buyer and seller automatically verified and executed via a computer network. Smart contracts deployed to Blockchains render transactions traceable, transparent, and irreversible.

As just one example, smart contracts could eliminate the so-called procure-to-pay gaps. When a product arrives and is scanned at a warehouse, a smart contract could immediately trigger requests for the required approvals and, once obtained, immediately transfer funds from the buyer to the seller. Sellers would get paid faster and no longer need to engage in dunning, and buyers would reduce their account payable costs. This could impact working capital requirements and simplify finance operations for both parties. On the enforcement side, a smart contract could be programmed to shut off access to an internet-connected asset if a payment is not received. For example, access to certain content might automatically be denied if payment was not received.

4.2 The Interplay With Traditional Text Agreements

One of the difficulties with discussing smart contracts is that the term is used to capture two very different paradigms. The first involves smart contracts that are created and deployed without any enforceable text-based contract behind them. For example, two parties reach an oral understanding as to the business relationship they want to capture and then directly reduce that understanding into executable code. We refer to these below as "code-only smart contracts." The second paradigm involves the use of smart contracts as vehicles to effectuate certain provisions of a traditional text-based contract, in which the text itself references the use of the smart contract to effectuate certain provisions. We refer to these as "ancillary smart contracts."

4.3 How smart contract work

"Smart contracts" is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a Blockchain-based platform. As discussed further below, the code can either be the sole manifestation of the agreement between the parties or might complement a traditional text-based contract and execute certain provisions, such as transferring funds from Party A to Party B. The code itself is replicated across multiple nodes of a Blockchain and, therefore, benefits from the security, permanence and immutability that a Blockchain offers. That replication also means that as each new block is added to the Blockchain, the code is, in effect, executed. If the parties have indicated, by initiating a transaction, that certain parameters have been met, the code will execute the step triggered by those parameters. If no such transaction has been initiated, the code will not take any steps. Most smart contracts are written in one of the programming languages directly suited for such computer programs, such as Solidity.

At present, the input parameters and the execution steps for a smart contract need to be specific and objective. In other words, if "x" occurs, then execute step "y." Therefore, the actual tasks that smart contracts are performing are fairly rudimentary, such as automatically moving an amount of cryptocurrency from one party's wallet to another when certain criteria are satisfied. As the adoption of Blockchain spreads, and as more assets are tokenized or go "on chain," smart contracts will become increasingly complex and capable of handling sophisticated transactions. Indeed, developers already are stringing together multiple transaction steps to form more complex smart contracts. Nonetheless, we are, at the very least, many years away from code being able to determine more subjective legal criteria, such as whether a party satisfied a commercially reasonable efforts standard or whether an indemnifications clause should be triggered and the indemnity paid.

Before a compiled smart contract actually can be executed on certain Blockchains, an additional step is required, namely, the payment of a transaction fee for the contract to be added to the chain and executed upon. In the case of the Ethereum Blockchain, smart contracts are executed on the Ethereum Virtual Machine (EVM), and this payment, made through the ether cryptocurrency, is known as "gas." The more complex the smart contract (based on the transaction steps to be performed), the more gas that must be paid to execute the smart contract. Thus, gas currently acts as an important gate to prevent overly complex or numerous smart contracts from overwhelming the EVM.

Smart contracts are presently best suited to execute automatically two types of "transactions" found in many contracts: (1) ensuring the payment of funds upon certain triggering events and (2) imposing financial penalties if certain objective conditions are not satisfied. In each case, human intervention, including through a trusted escrow holder or even the judicial system, is not required once the smart contract has been deployed and is operational, thereby reducing the execution and enforcement costs of the contracting process.

4.4 Benefits of Smart Contracts

4.3.1 Accuracy, Speed, and Efficiency

The contract is immediately executed when a condition is met. Because smart contracts are digital and automated, there is no paperwork to deal with, and no time was spent correcting errors that can occur when filling out documentation by hand. Smart contracts use software code to automate tasks, thereby reducing the time it takes to maneuver through all the human interaction related processes. Because everything is coded, the time taken to do all the work is the time taken for the code in the smart contract to execute.

4.3.2 Trust and Transparency

There's no need to worry about information being tampered with for personal gain because there's no third party engaged and encrypted transaction logs are exchanged among participants. The smart contract can't be lost as its embedded in the Blockchain itself.

4.3.3 Security

Because Blockchain transaction records are encrypted, they are extremely difficult to hack. Furthermore, because each entry on a distributed ledger is linked to the entries before and after it, hackers would have to change the entire chain to change a single record.

4.3.4 Savings

Smart contracts eliminate the need for intermediaries to conduct transactions, as well as the time delays and fees that come with them.

4.3.5 Autonomy

There is no third part involved. The contract is made by you and shared between the parties. No intermediaries involved which minimizes bullying and grants fully authority to the dealing parties. Also, the smart contract is maintained and executed by all the nodes on the network, thus removing all the controlling power from any one party's hand.

4.5 Applications of Smart Contracts

4.5.1 Smart Contacts and Flight Insurance

Let's consider a real-life scenario in which smart contracts are used. Rachel is at the airport, and her flight is delayed. AXA, an insurance company, provides flight delay insurance utilizing Ethereum smart contracts. This insurance compensates Rachel in such a case. How? The smart contract is linked to the database recording flight status. The smart contract is created based on terms and conditions.

The condition set for the insurance policy is a delay of two hours or more. Based on the code, the smart contract holds AXA's money until that certain condition is met. The smart contract is submitted to the nodes on EMV (a runtime compiler to execute the smart contract code) for evaluation. All the nodes on the network executing the code must come to the same result. That result is recorded on the distributed ledger. If the flight is delayed in excess of two hours, the smart contract self-executes, and Rachel is compensated. Smart contracts are immutable; no one may alter the agreement.

4.5.2 Voting and Blockchain Implementation of Smart Contracts

Using Blockchain in the voting process can eliminate common problems. A centralized voting system faces difficulties when it comes to tracking votes – identity fraud, miscounts, or bias by voting officials. Using a smart contract, certain predefined terms and conditions are pre-set in the contract. No voter can vote from a digital identity other than his or her own. The counting is foolproof. Every vote is registered on a Blockchain network, and the counting is tallied automatically with no interference from a third party or dependency on a manual process. Each ID is attributed to just one vote. Validation is accomplished by the users on the Blockchain network itself. Thus, the voting process can be in a public Blockchain, or it could be in a decentralized autonomous organization-based Blockchain setup. As a result, every vote is recorded on the ledger, and the information cannot be modified. That ledger is publicly available for audit and verification.

Smart contracts allow you to create voting systems in which you can add and remove members, change voting rules, change debating periods, or alter the majority rule. For instance, you can create a vote for a decision within a decentralized autonomous organization. Rather than a central authority making a decision, a voting mechanism within the organization can determine whether the proposal is accepted or rejected.

4.5.3 Blockchain Implementation of a Smart Contract and Crowdfunding

Ethereum-based smart contracts may be used to create digital tokens for performing transactions. You may design and issue your own digital currency, creating a tradable computerized token. The tokens use a standard coin API. In the case of Ethereum, there are standardizations of ERC 2.0, allowing the contract to access any wallet for exchange automatically. As a result, you build a tradable token with a fixed supply. The platform becomes a central bank of sorts, issuing digital money.

Suppose you want to start a business requiring funding. But who would lend money to someone they don't know or trust? Smart contracts have a major role to play. With Ethereum, you can build a smart contract to hold a contributor's funds until a given date passes or a goal is met. Based on the result, the funds are released to the contract owners or sent back to the contributors. The centralized crowdfunding system has many issues with management systems. To combat this, a DAO (Decentralized Autonomous Organization) is utilized for crowdfunding. The terms and conditions are set in the contract, and every individual participating in crowdfunding is given a token. Every contribution is recorded on the Blockchain.

4.5.4 Safeguarding the efficacy of medications

Sonoco and IBM are working to reduce issues in the transport of lifesaving medications by increasing supply chain transparency. Powered by IBM Blockchain Transparent Supply, Pharma Portal is a Blockchain-based platform that tracks temperature-controlled pharmaceuticals through the supply chain to provide trusted, reliable and accurate data across multiple parties.

4.5.5 Increasing trust in retailer-supplier relationships

The Home Depot uses smart contracts on Blockchain to quickly resolve disputes with vendors. Through real-time communication and increased visibility into the supply chain, they are building stronger relationships with suppliers, resulting in more time for critical work and innovation.

4.5.6 Making international trade faster and more efficient

By joining we. trade, the trade finance network convened by IBM Blockchain, businesses are creating an ecosystem of trust for global trade. As a Blockchain-based platform, we. trade uses standardized rules and simplified trading options to reduce friction and risk while easing the trading process and expanding trade opportunities for participating companies and banks.

4.6 Use Cases of Smart Contracts

The use cases for smart contracts range from simple to complex.

They can be used for simple economic transactions, such as moving money from point A to point B, as well as for smart access management in the sharing economy.

Smart contracts could disrupt many industries.

Banking, insurance, energy, e-government, telecommunications, the music business, art, mobility, education, and many other industries have use cases.

Below table shows, the difference between 3 types of Use-Cases of Smart Contracts that are Technical Use-Cases, Legal Use-Cases and Economic Use-Cases:

Technical Use-Cases	**Legal Use-Cases**	**Economic Use-Cases**
Self-verifying Self-executing	It can map legal obligations into an automated process.	Higher transparency Fewer intermediaries

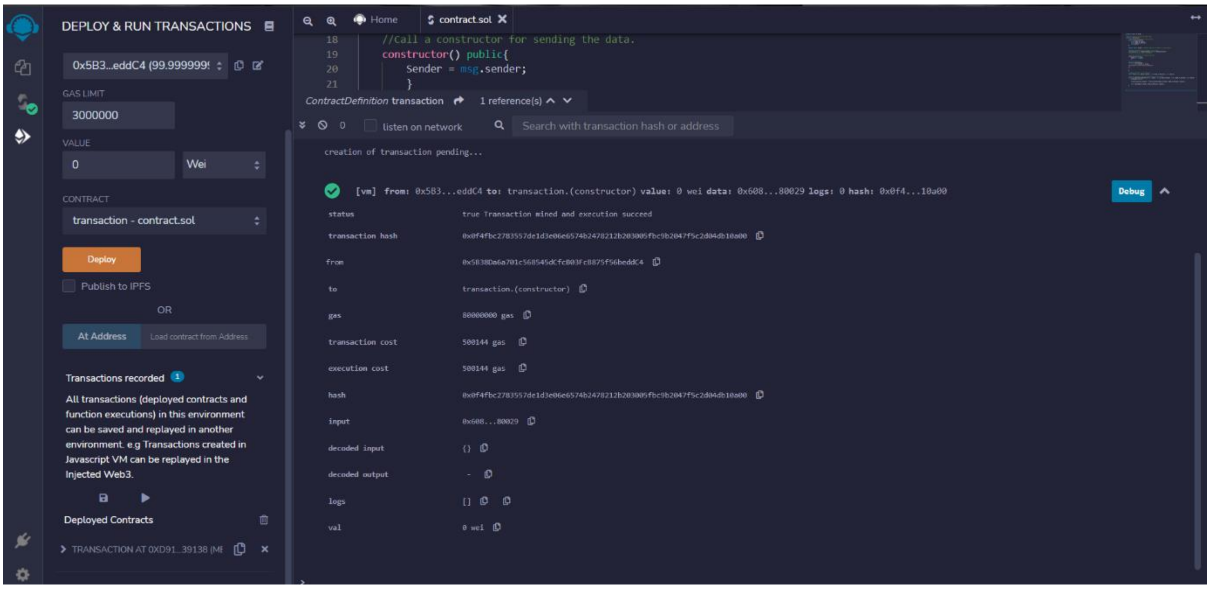
Tamper resistance	If implemented correctly, they can provide a greater degree of contractual security	Lower transaction costs

Table 4.1: Technical Use-Cases vs Legal Use-Cases vs Economic Use-Cases

4.7 Money Transaction Smart Contract

Here is one deployed smart contract of money transfer from one person to another person. Here, one is sender and other one is receiver, the transaction that is performed between them is the transfer of money from sender to receiver.

Below figure shows the deployment details and transaction details of the deployed smart contract:


DEPLOY & RUN TRANSACTIONS
Home
contract.sol
Deploy
At Address
Load contract from Address
Debug
OR
Search with transaction hash or address

0x5B3...eddC4 (99.999999!

GAS LIMIT
3000000

VALUE
0 Wei

CONTRACT
transaction - contract.sol

☐ Publish to IPFS

Transactions recorded 1

All transactions (deployed contracts and function executions) in this environment can be saved and replayed in another environment. e.g Transactions created in Javascript VM can be replayed in the Injected Web3.

Deployed Contracts

TRANSACTION AT 0XD91...39138 (ME

```
    //Call a constructor for sending the data.
    constructor() public{
        Sender = msg.sender;
        }
```

ContractDefinition transaction 1 reference(s)

0 ☐ listen on network

```
creation of transaction pending...

[vm] from: 0x5B3...eddC4 to: transaction.(constructor) value: 0 wei data: 0x608...80029 logs: 0 hash: 0x0f4...10a00
status              true Transaction mined and execution succeed
transaction hash    0x0f4fbc2783557de1d3e06e6574b2478212b203005fbc9b2047f5c2d04db10a00
from                0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                  transaction.(constructor)
gas                 80000000 gas
transaction cost    500144 gas
execution cost      500144 gas
hash                0x0f4fbc2783557de1d3e06e6574b2478212b203005fbc9b2047f5c2d04db10a00
input               0x608...80029
decoded input       {}
decoded output       -
logs                []
val                 0 wei
```

Fig 4.1: Deployed Smart Contract

CHAPTER 5

SUSTAINABLE DEVELOPMENT GOALS

5.1 What are Sustainable Development Goals

The 2030 Agenda for Sustainable Development, adopted by all United Nations Member States in 2015, provides a shared blueprint for peace and prosperity for people and the planet, now and into the future. At its heart are the 17 Sustainable Development Goals (SDGs), which are an urgent call for action by all countries - developed and developing - in a global partnership. They recognize that ending poverty and other deprivations must go hand-in-hand with strategies that improve health and education, reduce inequality, and spur economic growth – all while tackling climate change and working to preserve our oceans and forests.

The Sustainable Development Goals (SDGs) or Global Goals are a collection of 17 interlinked global goals designed to be a "blueprint to achieve a better and more sustainable future for all". The SDGs were set up in 2015 by the United Nations General Assembly (UN-GA) and is intended to be achieved by 2030. They are included in a UN-GA Resolution called the 2030 Agenda or what is colloquially known as Agenda 2030. The SDGs were developed in the Post-2015 Development Agenda as the future global development framework to succeed the Millennium Development Goals which were ended in 2015.

The Sustainable Development Goals (SDGs), also known as the Global Goals, were adopted by the United Nations in 2015 as a universal call to action to end poverty, protect the planet, and ensure that by 2030 all people enjoy peace and prosperity.

The 17 SDGs are integrated—they recognize that action in one area will affect outcomes in others, and that development must balance social, economic and environmental sustainability.

Countries have committed to prioritize progress for those who're furthest behind. The SDGs are designed to end poverty, hunger, AIDS, and discrimination against women and girls.

The creativity, knowhow, technology and financial resources from all of society is necessary to achieve the SDGs in every context.

The 17 SDGs are:

(1) No Poverty

(2) Zero Hunger

(3) Good Health and Well-being

(4) Quality Education

(5) Gender Equality

(6) Clean Water and Sanitation

(7) Affordable and Clean Energy

(8) Decent Work and Economic Growth

(9) Industry, Innovation and Infrastructure

(10) Reduced Inequality

(11) Sustainable Cities and Communities

(12) Responsible Consumption and Production

(13) Climate Action

(14) Life Below Water

(15) Life On Land

(16) Peace, Justice, and Strong Institutions

(17) Partnerships for the Goals.

Though the goals are broad and interdependent, two years later (6 July 2017) the SDGs were made more "actionable" by a UN Resolution adopted by the General Assembly. The resolution identifies specific targets for each goal, along with indicators that are being used to measure progress toward each target. The year by which the target is meant to be achieved is usually between 2020 and 2030. For some of the targets, no end date is given.

To facilitate monitoring, a variety of tools exist to track and visualize progress towards the goals. All intention is to make data more available and easily understood.[5] For example, the online publication SDG Tracker, launched in June 2018, presents available data across all indicators. The SDGs pay attention to multiple cross-cutting issues, like gender equity, education, and culture cut across all of the SDGs. There were serious impacts and implications of the COVID-19 pandemic on all 17 SDGs in the year 2020.

5.2 Industry, Innovation and Infrastructure

Blockchain is going to achieve all these targets sooner or later and will help in achieving 9th Sustainable Environment Goal i.e., Industry, Innovation and Infrastructure.

A functioning and resilient infrastructure is the foundation of every successful community. To meet future challenges, our industries and infrastructure must be upgraded. For this, we need to promote innovative sustainable technologies and ensure equal and universal access to information and financial markets. This will bring prosperity, create jobs and make sure that we build stable and prosperous societies across the globe.

5.2.1 The Targets

Everyone can help to make sure that we meet the Global Goals. Use these eight targets to create action to build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation.

- **Target 1- Develop Sustainable, Resilient And Inclusive Infrastructures**

Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.

- **Target 2- Promote Inclusive And Sustainable Industrialization**

Promote inclusive and sustainable industrialization and, by 2030, significantly raise industry's share of employment and gross domestic product, in line with national circumstances, and double its share in least developed countries.

- **Target 3- Increase Access To Financial Services And Markets**

Increase the access of small-scale industrial and other enterprises, in particular in developing countries, to financial services, including affordable credit, and their integration into value chains and markets.

- **Target 4- Upgrade All Industries And Infrastructures For Sustainability**

By 2030, upgrade infrastructure and retrofit industries to make them sustainable, with increased resource-use efficiency and greater adoption of clean and environmentally sound technologies and industrial processes, with all countries taking action in accordance with their respective capabilities.

- **Target 5- Enhance Research And Upgrade Industrial Technologies**

Enhance scientific research, upgrade the technological capabilities of industrial sectors in all countries, in particular developing countries, including, by 2030, encouraging innovation and substantially increasing the number of research and development workers per 1 million people and public and private research and development spending.

- **Target 6- Facilitate Sustainable Infrastructure Development For Developing Countries**

Facilitate sustainable and resilient infrastructure development in developing countries through enhanced financial, technological and technical support to African countries, least developed countries, landlocked developing countries and small island developing States.

- **Target 7- Support Domestic Technology Development And Industrial Diversification**

Support domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification and value addition to commodities.

- **Target 8- Universal Access To Information And Communications Technology**

Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020.

5.3 How Blockchain helps to achieve the SDGs

Blockchain have application regarding the SDGs in different ways:

- providing all actors, roles and participants in general with a layer of traceability and global transparency, which inherently promotes the behavior and responsible use of resources of all kinds.

- offering resilience and security capabilities, which hinder any kind of unilateral manipulation that may harm third parties.

- guaranteeing the precision in the surveillance of actions through the use of smart contracts, which validate the actions that occur within Blockchain.

All this makes Blockchain the fastest, most economical, resilient and fair technological alternative for all the actors involved in each of the SDGs.

ODS initiatives based on Blockchain

Climate change (SDG 13: Climate Action) is configured as the key objective of this program for the development of Blockchain-based innovations. The UN believes that the application of Blockchain to this extent can achieve, among others, the following benefits:

- Strengthening of monitoring and verification of the impacts of the actions undertaken.

- Improvement of transparency, traceability and cost-effectiveness.

- Building trust among environmental actors.

- Creation of mechanisms that encourage climate action, especially in an accessible way to the poorest.

- Mobilization of green finance.

Another good example is occurring in several Latin American countries, with the implementation of different initiatives aimed at the fight against poverty (SDG 1: End of Poverty) based on Blockchain. In these cases, access to basic services is facilitated without the cost overruns of the less favored, by providing them with a digital identity with which to access them.

Blockchain enables, as we have said, a transparent and secure traceability, which ensures that the products we consume have not been produced in circumstances of human exploitation, such as the use of minors or enslaving wages. This also always has an effect on an increase in the flow of financing for disadvantaged sectors, as it has the immutable guarantee of ethical behavior throughout the entire production chain (SDG 8: Decent Work and Economic Growth and SDG 12: Responsible Production and Consumption). Fair trade is, therefore, one of the beneficiaries of this use of Blockchain.

The unique medical history as the property of the citizen is another of the rights of any person. Blockchain will allow us to have this benefit (SDG 3: Health and Wellness).

Finally, regarding energy saving and pollution reduction (SDG 7: Affordable and Non-Pollutant Energy), applications are being created that allow traceability to be obtained on obtaining and origin of energy, as well as enabling CO2 footprint management generated by companies, allowing to implement bonus programs using tokens.

CHAPTER 6

CONCLUSION

Overall, the conclusion stated that some consensus algorithms used in Blockchain have been highlighted, which are categorized into two main kinds: proof-based and vote-based consensus algorithms. In the former, nodes have to show they have performed sufficient proof to get the right to do the appending work, and get the rewards. Meanwhile, in the latter, nodes will exchange messages with others to make an agreement about the blocks or transactions to be appended to the ledger. We also make comparisons between these two types based on some of their highlighted characteristics, which illustrates the advantages and drawbacks of each category. It could be observed that besides the original public Blockchain with proof-based consensus algorithms, the newly developed consortium and private Blockchain has much potential with vote-based ones at this time.

Gone are the days when Blockchain networks just had a handful of protocols to achieve consensus. Though Proof of Work and Proof of Stake still remain the most popular consensus mechanisms, it is essential that we question their accountability in diverse applications. As of now, the world seems to be advancing towards different consensus algorithms to tailor the needs of different applications. By the means of this survey, we deduce that although no algorithm could be deemed as the most superior algorithm, it depends on the nature of the application to find the single best consensus protocol - like whether the Blockchain is public or private, performance and throughput needs, project scale etc. Nonetheless, this survey shows how much of an impact Blockchain-based consensus algorithms are creating to empower decentralisation and to root out the centralised means of going about things.

The distributed ledger, a disruptive technology, powered by consensus protocols, with its adaptability and application has revolutionized the business processes. In this paper, we surveyed and analyzed a few consensus protocols. No consensus protocol is being perfect, and there are always certain trade-offs related to performance, security, and scalability efficiency. Each of these protocols provides domain-specific solutions and serves different purposes in spite of having their strengths and weaknesses. Above all, they all serve as a common solution for one of the main problems of distributed ledger, i.e., double-spending. Presently, the trend is shifting towards a hybrid approach; that is, implementation will be based on two or more consensus protocols. The consensus protocol, the backbone of a Blockchain, comes in varied implementations to serve different use cases. Since the inception of the first consensus protocol, i.e., Proof of Work, researchers are working to develop a scalable, efficient, and secure consensus protocol that could produce excellent results and could help in the growth of the economy and infrastructure.

REFERENCES

1. https://www.ibm.com/in-en/topics/what-is-Blockchain
2. https://www.investopedia.com/terms/b/Blockchain.asp
3. https://en.wikipedia.org/wiki/Ledger
4. https://en.bitcoin.it/wiki/Block
5. https://en.bitcoin.it/wiki/Genesis_block
6. https://en.wikipedia.org/wiki/Digital_currency
7. Public Vs. Private Blockchain : A Comprehensive Comparison (Blockchain-council.org)
8. https://101Blockchains.com/history-of-Blockchain-timeline/
9. Cachin, C.: Architecture of the hyperledger Blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310, no. 4 (2016)
10. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J.J.: Blockchain contract: a complete consensus using Blockchain. In: 2015 IEEE 4th global conference on consumer electronics (GCCE), pp. 577–578. IEEE (2015)
11. Divya, M., Biradar, N.B.: IOTA-next generation block chain. Int. J. Eng. Comput. Sci. 7(04), 23823–23826 (2018)
12. Schwartz, D., Youngs, N., Britto, A., et al., 2014. The Ripple Protocol Consensus Algorithm. Ripple Labs Inc White Paper 5
13. Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M., 2014. Proof of activity: extending bitcoin's proof of work via proof of stake. In: IACR Cryptology ePrint Archive 2014, p. 452.
14. M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," ACM Transactions on Computer Systems, vol. 20, no. 4, pp. 398–461, Nov. 2002
15. F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of Blockchain-based applications: Current status, classification and open issues", Telematics Inform., vol. 36, pp. 55-81, Mar. 2019
16. Stuart Haber and W. Scott Stornetta, "How to time-stamp a digital document" Journal of Cryptology, volume 3, pages 99–111, 1991.
17. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
18. L. Lamport et al., Paxos made simple, ACM Sigact News 32(4) (2001), 18-25. https://docs.wavesplatform.com/en/Blockchain/leasing#leasing-benefits-for-the-tokenholder
19. S. Zoican, M. Vochin, R. Zoican and D. Galatchi, Blockchain and Consensus Algorithms in Internet of Things, ISETC, pp. 1-4, 2018.
20. S. J. Alsunaidi and F. A. Alhaidari, A Survey of Consensus Algorithms for Blockchain Technology, 2019, ICCIS, pp. 1-6, 2019.
21. W. Wang, A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks, IEEE Access 7 (2019), 22328-22370
22. S. Zhanga and J.-H. Lee, Analysis of the main consensus protocols of Blockchain, https://doi.org/10.1016/j.icte.2019.08.001, 2019.
23. M. Salimitari, M. Chatterjee, and Y. P. Fallah, "A survey on consensus methods in Blockchain for resource-constrained IoT networks," Internet of 6ings, vol. 11, 2020
24. S. Bamakan, A. Motavali, and A. Bondarti, "A survey of Blockchain consensus algorithms performance evaluation criteria," Expert Systems with Applications, vol. 154, 2020.
25. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of Blockchain. IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2567-2572. 10.1109/SMC.2017.8123011
26. Ishan, P. B., & Rai, G. (2018). Analysis of Cryptographic Hash in Blockchain for Bitcoin Mining Process. International Conference on Advances in Computing and Communication Engineering (ICACCE), 105-110. 10.1109/ICACCE.2018.8441688

27. Chalaemwongwan, N., & Kurutach, W. (2018). State of the art and challenges facing consensus protocols on Blockchain. International Conference on Information Networking (ICOIN), 957-962. 10.1109/ ICOIN.2018.8343266
28. Tasatanattakool, P., & Techapanupreeda, C. (2018). Blockchain: Challenges and applications. International Conference on Information Networking (ICOIN), 473-475.
29. Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C., & Njilla, L. (2017). Consensus protocols for Blockchain-based data provenance: Challenges and opportunities. IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 469-474
30. Wang, Y., Cai, S., Lin, C., Chen, Z., Wang, T., Gao, Z., & Zhou, C. (2019). Study of Blockchains's Consensus Mechanism Based on Credit. IEEE Access: Practical Innovations, Open Solutions, 7, 10224–10231. doi:10.1109/ACCESS.2019.2891065
31. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE International Congress on Big Data (BigData Congress), 557-5
32. Eyal, I. and Sirer, E.G. "Majority is not enough: Bitcoin mining is vulnerable". International Conference on Financial Cryptography and Data Security pages 436–454. March, 2014.
33. H. Cho, "Asic-resistance of multi-hash proof-of-work mechanisms for Blockchain consensus protocols," IEEE Access, vol. 6, pp. 66210–66222, 2018
34. S. Sayeed and H. Marco-Gisbert, "Assessing Blockchain consensus and security mechanisms against the 51% attack," Applied Sciences, vol. 9, no. 9, p. 1788, 2019
35. R. Fitri Sari, "Evaluation of proof of work (pow) Blockchains security network on selfish mining," 2018
36. L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," 2017
37. M. Castro and B. Liskov, "Practical byzantine fault tolerance," OSDI, vol. 99, pp. 173–186, 1999.
38. M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," ACM Transactions on Computer Systems, vol. 20, no. 4, pp. 398–461, 2002.
39. M. Snider, K. Samani, and T. Jain, "Delegated proof of stake: features & tradeoffs," 2018
40. Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang, and Li He, "A comparative study of Blockchain consensus algorithms," Journal of Physics: Conference Series, vol. 1437, 2020
41. Christofi, G. (2019, October). Study of consensus protocols and improvement of the Delegated Byzantine Fault Tolerance (DBFT) algorithm (Projecte Final de Màster Oficial). UPC, Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona, Departament d'Enginyeria Telemàtica. Retrieved from http://hdl.handle.net/2117/171243
42. Alsunaidi, S. J., & Alhaidari, F. A. (2019, April). A survey of consensus algorithms for Blockchain technology. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE
43. Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of Blockchain consensus algorithms. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1545-1550). IEEE
44. Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016, December). Proof of luck: An efficient Blockchain consensus protocol. In proceedings of the 1st Workshop on System Software for Trusted Execution (pp. 1-6).