[1] **Shekhawat Pradeep**

[2] **Gopal Krishan Prajapat**

[3] **Dharmendra Yadav**

A Comprehensive Review of Blockchain Infrastructure: Insights into Architecture, Consensus Algorithms, and Development Frameworks

Abstract: **-** Blockchain is a replicated data structure that consists of multiple blocks connected through hash values. Cryptography serves as the backbone to Blockchain technology, as it ensures that blocks are interconnected through hash values. Additionally, Consensus algorithms are essential for endorsing and verifying blocks and transactions, promoting cooperation and collaboration in a trustless system, and maintaining consistency in the state of the blockchain. The aim of this study is to give a summary of the history and architecture of Blockchain technology, followed by a comparative analysis of consensus algorithms and frameworks. Through this study, our aim is to present a complete overview of the various consensus algorithms and frameworks built upon the Blockchain technology, which can enable stakeholders to take appropriate decisions when implementing blockchain-based solutions to address various problems.

Keywords: Blockchain, Smart Contracts, Consensus Algorithms, Distributed Ledger, Decentralized Network, Blockchain Frameworks.

I. INTRODUCTION

A Blockchain technology with promising features such as tamper proof, transparency, trustless decentralization, pseudonymity, trackability of data and fault-tolerance is a way of storing the data in secure manner in form of blocks connected through a hash value obtained by applying the cryptographically secured collision-resistant hash function[1]. It is just like a decentralized ledger or replicated data structure where data can be captured. To maintain consistency the ledger is distributed across the nodes and common decision is considered before the data is added to it. The Distribution of ledger across the nodes, validating and verifying the data, and reaching to a common decision or agreement before adding the date to the ledger such tasks are performed by the consensus algorithms under peer-to-peer network in which each node has equal privileges. The consensus mechanism guarantees that every node in a distributed network maintains the same data at any time in the distributed ledger. Blockchain technology is useful when multiple stakeholders such as Organizations, Industries or People do not trust one another, but they want to cooperate, collaborate, or coordinate for achieving the common goal. Many researchers have been investigating various domains in which blockchain technology can be applied, including Healthcare industry, Digital Identity management, Supply Chain management, Telecommunication sectors, Cryptocurrency, Internet of thing, Smart farming etc. [2], [3], [4], [5], [6]. All these blockchain based applications in various domains use consensus algorithms and frameworks for providing the solution to a problem. Blockchain framework is a program that provides tools and necessary infrastructures to build and deploy Blockchain based applications. The objective of this work is to enable stakeholders such as Researcher, industrial, and academician to apply appropriate consensus algorithm and framework for implementing the blockchain based solution. This study comprises of 1) Overview of Blockchain history, 2) Architecture of Blockchain, 3) Consensus algorithms and their comparative analysis 4) Blockchain frameworks and their comparative analysis.

II. OVERVIEW OF HISTORY

Wherever In 1991, Stuart Haber and Scott Stornetta proposed the concept of securing the chain of blocks for digitally timestamping of documents to detect documents tempering [7]. In this idea, instead of storing the document directly, A cryptographically secured collision-resistant hash function is applied on document, time stamp, sequence

[1] Department of Computer Science and Engineering, Bikaner Technical University, Bikaner, Rajasthan-334001, India.
Email: pradeep.shekhawat@bkbiet.ac.in

[2] Department of Computer Science and Engineering, Bikaner Technical University, Bikaner, Rajasthan-334001, India.
Email: krishan3629@gmail.com

[3] Department of Computer Science and Engineering, Bikaner Technical University, Bikaner, Rajasthan-334001, India.
Email: dyadav@cet-gov.ac.in

no assigned to a request when it was made, client-Id, and hash value of previous request to obtain a hash value through which next block is connected. In 1992, these scientists included the Merkle tree in their design to allow several certificates to be collected into one block and single hash value could be generated out of the root of the Merkle tree [8]. Before cryptocurrency come into existence, David Chaum in 1983 introduced the digital based eCash System to protect people's privacy when sending money. The key aspect of ecash was based on blind signature in which contents of messages were hidden before signing resulting in no one was able to see the amount of transaction and whom the transaction was directed to. In 1989, ecash was implemented via DigiCash company started by Dr David chaum [9]. The digital currency management was the major concerned in ecash system. Users of the ecash system first purchase digital currency from a bank, which then issues them with a special identification code for each digital currency they own. Then, without hiding the identity of users, these digital funds can be anonymously and securely spent. When users want to use a digital currency, they hand it to the intended receiver, who then contacts the bank that issued it to confirm its validity. The bank then verifies the digital currency and transfers the necessary sums to the beneficiary while keeping the identity of the user hidden. In ecash system, a bank served as a reliable third party that gave users privacy and protection while also guarding against fraud and other illegal activities. The bank oversaw approving transactions, keeping track of digital currency, and guaranteeing the system's general integrity. The ecash system didn't get popularized among the people therefore the company went bankrupt in 1998.

While the requirement for a centralized third party like a bank has been eliminated by modern blockchain-based cryptocurrencies like Bitcoin (BTC) and Ether (ETH), the principles and concepts of digital cash in the ecash system have had an impact on the creation of modern cryptocurrencies and digital payment systems. In 2009, "Bitcoin: A Peer-to-Peer Electronic Cash System" was invented by Satoshi Nakamoto, an anonymous individual or collective whose identity is not known [1]. The purpose of this invention was to overcome the issue of double spending by utilizing a peer-to-peer network, to remove the reliance on trusted intermediaries like banks, and to solve the management issues associated with digital currencies in the eCash system. The blockchain got popularized after the invention of Bitcoin. As a digital currency, it runs on a decentralized peer-to-peer network, which means that transactions are handled and confirmed by a distributed network of computing devices instead of relying on centralized organization like a bank. Unlike traditional currencies, Bitcoin does not fall under the control of any trusted intermediaries like banks and governments. It relies on a public ledger known as the Blockchain that is sustained by a distributed network of computers for transaction verification and recording. Bitcoin's functionality can be described in terms of Transactions, Mining process and Digital Wallet.

1. Transaction: It is made and broadcasted across the network whenever one node wishes to send Bitcoins to another node. In addition to the public encryption key of the sender and the private decryption key of the receiver, the amount to be sent, the transaction fees given to incentivize miners for inclusion of transactions into the block, script itself are all contained within each transaction. The network nodes then use a consensus procedure to verify that the transaction is valid before approving it. When a Bitcoin transaction is approved, a newly validated block is integrated to the blockchain, which is a continuously growing list of previously validated blocks. With reference to the preceding block embedded in each new block, the blockchain forms an unbreakable chain of transactions [10].

2. Mining: Mining encourages network participation and transaction verification. Miners get Bitcoins when they solve complex mathematical problems with powerful computers. Changing the blockchain requires a lot of processing power, this produces a secure network that resists fraud and manipulation [10].

3. Digital Wallet: Computer and phone wallets hold bitcoins. Each wallet's private key signs transactions and proves Bitcoin ownership. Bitcoin is a safe, decentralized way to transfer currency. Proof of Work (PoW) and encryption assure transaction integrity, authenticity, non-repudiation, and confidentiality.

A. Evaluation of Blockchain

Over the years, the evaluation of Blockchain technology has undergone significant development. The various stages in the evaluation of Blockchain technology are depicted in Figure 1 with detail description is explained below:

1. Blockchain 1.0: It refers to the first generation of Blockchain Technology which mainly focuses on creation and use of cryptocurrencies [11]. Its key aspects include consensus algorithms, decentralized ledger that is replicated

across peers (i.e Nodes) in peer-to-peer (P2P) network for recording the transactions and P2P network that allows nodes to interact with one another in decentralized fashion.

2. Blockchain 2.0: This phase involves blockchain evolving beyond the use of cryptocurrency [11]. While the initial phase of blockchain technology was dedicated mainly to creating a decentralized cryptocurrency, Blockchain 2.0 aims to extend its capabilities by incorporating a more diverse set of decentralized applications (dApps) and use cases. One of the key aspects of this phase is that it uses smart contracts. They are similar to traditional contracts consisting of various terms and conditions between different parties. These terms and conditions are automatically triggered once the specified criteria are met. They allow automated trust-less transactions between parties without the involvement of intermediaries. Various blockchain based applications are adopting self-executing smart contracts, including supply chain management system, voting systems, and financial services, among others. In this Phase, Different solutions have been provided by the researchers for solving the scalability issues encountered in Blockchain 1.0 such as sharding as on chain solution and non-on-chain solutions including the payment channels, side chains and state channels.

a. Sharding: It divides the blockchain's network into smaller groups of nodes where each group is considered as shard. In this, Blockchain's data is divided into subsets of data which are distributed among different shards for faster and more efficient processing. Each shard can process the transactions independently enabling more volume of transactions to be processed in parallel while compromising with serval factors effecting the performance and security aspects of Blockchain including interoperability, performance, complexity, replication and centralization [12].

b. Sidechain or layer-2 Solution: A sidechain is created as a separate chain using a 2-way peg technique to execute more transactions in parallel and transfer more assets between the main blockchain and the sidechain. This technique provides privacy, interoperability, and scalability features but can compromise decentralization if the sidechain is governed by an entity or group. Each side chain may have its own token, consensus protocol and security irrespective of main blockchain. The blockchain design may allow multiple sidechains to be connected to main blockchain also known as parent blockchains [13].

c. State Channel: It is a process in which multiple parties transact with one another off the main blockchain, while still maintaining the security provided by the underlying network. Instead of recording all the transactions that took place between multiple parties to main blockchain, only some of the transactions are recorded on it and only states of rest of transaction are maintained. This can be achieved through Smart Contract [14].

d. Payment Channel: To increase throughput of transactions and to reduce the transaction fees, transactions between multiple parties are not stored in Blockchain, instead they are recorded on the payment channel itself. It is derived from State channel [15].

e. Interoperability: It is a process of enabling different Blockchain networks to exchange information and assets, data sharing and cross-chain communication between them. Interoperability can be achieved by developing cross chain smart contracts, creating standard protocols for data exchange, and building the bridges between different blockchains [16].

3. Blockchain 3.0: In this phase, different technologies have been purposed to take care of the issues pertaining to Security, Privacy and Decentralization parameters.

a. Security: To achieve Security new cryptographic techniques such as homomorphic encryption has been developed for storing and sharing the data securely on the blockchain [17].

b. Privacy: To achieve anonymous and private transactions on the blockchain, a new cryptography technique named zero-knowledge proofs has been introduced [18], [19].

c. Decentralization: To cope with decentralization a smart contract enabled blockchain based technology named Decentralized Autonomous Organization (DAO) has been proposed. The working of DAO is based on a set of rules and policies made by its stakeholders who are the members of the organization who have power to vote. Encoding the set of rules and policies as smart contracts in blockchain technology gives the power to individual members to be involved in decision making process and resource allocation based on voting system [20].

Frequently used Projects based on Blockchain 3.0 are described below:

d. Ethereum 2.0: To increase the throughput of transactions, this platform uses Proof of stake (PoS) consensus algorithm which is a replacement over Proof of work (PoW) consensus algorithm used by the early version of Ethereum and sharding technique [21].

e. Cardano: This open-source system integrates a blockchain platform with smart contract and Ouroboros consensus mechanism that is a specific implementation of PoS consensus algorithm, to address the Energy consumption and scalability issues. In each round, a leader that is responsible for creation of block and validation of transaction is selected using verifiable random functions [22].

f. Polkadot: This platform supports interoperability across multiple blockchains. It is designed to allow creation of a decentralized internet where blockchains can exchange messages and perform transactions without the need of intermediaries [23].

g. Oasis Network: To achieve privacy, This Blockchain based network uses homomorphic encryption for secure data storage and sharing on the blockchain. It also uses a PoS algorithm and a layered architecture for achieving scalability.

4. Blockchain 4.0: Blockchain technology has evolved to its fourth generation termed as Blockchain 4.0. Although blockchain 3.0 focused on tackling the scalability, security, privacy, and interoperability challenges of previous blockchain generations, blockchain 4.0 aims to incorporate Artificial Intelligence, Internet of things, Digital Identity, Energy Efficiency and Big Data to take advancements to the next level and radically alter our usage and interaction with blockchain technology. These technologies and features are depicted below:

a. Artificial Intelligence (AI): A decision-making process and automatic execution of terms of the agreement can be introduced in Smart Contract if AI and Blockchain are integrated together. The AI can analyze and predict the data stored on Blockchain to make prediction about future trends and to detect fraudulent activities in order to increase efficiency and security issues [24].

b. Internet of Things (IoT): This describes the interconnected network where physical devices, vehicles, and other objects are linked to the internet and capable of communication with one other. The Objective of Blockchain 4.0 is to integrate the IoT capabilities with the blockchain to enable secure and transparent communication between devices and the creation of more sophisticated applications [25].

c. Decentralized Finance (DeFi): DeFi uses blockchain technology to create decentralized financial applications without the need of traditional financial institutions. It uses Peer to Peer financial network to provide financial services to its users [26].

d. Digital Identity: To uniquely identify, verify and authenticate individual, organization and devices across the network digital identities are stored in decentralized manner to achieve security, transparency and privacy. Unlike centralized identity management system which has single point of control for managing and controlling the digital identities, decentralized identity management system uses Self-Sovereign Identity that enables individuals to have a self-control over personal information and decentralized identifiers [18].

e. Energy Efficiency: To deal efficiently with increasing demand of Blockchain Technology, Blockchain 4.0 aims to create more energy-efficient blockchain networks using new consensus algorithms and implementing energy-efficient mining algorithms [27].

Some examples of blockchain 4.0 projects include:

f. Hedera Hashgraph: To achieve high scalability and fast transaction processing, this platform utilizes a new consensus algorithm known as Hashgraph. It also integrates AI and IoT technology into its blockchain ecosystem [28].

g. Algorand: To achieve high scalability and energy efficiency, this platform utilizes a pure PoS consensus algorithm. It also integrates smart contract capabilities and digital identity technology into its blockchain ecosystem [29].

h. Solana: To achieve high scalability and fast transaction processing, this platform utilizes a new consensus mechanism called Proof of History (PoH). It also integrates DeFi and digital identity capabilities into its blockchain ecosystem [30].

i. EOS: Block.one Company released this open and decentralized platform in 2018 for running and building dApps. It uses stake EOS Cryptocurrencies as native tokens for its platform for electing the fixed number of block producers, resource allocation such as Bandwidth, CPU and storage for running dApps on the platform, and governance. The transaction fees are based on the resource allocation mechanism. It uses DPoS consensus mechanism to improve the transaction through put and scalability issues of PoW mechanism [31].

j. Ripple: It is a block chain-based platform which allows transfers of money between different countries i.e Cross-Border Transactions without the involvement of intermediaries. It uses XRP cryptocurrency as a token for faster settlement and lower transaction fees as compared to traditional currency exchanges methods and variant of DPoS for faster transaction processing times due to involvement of limited number of validators [32].

k. Binance Smart Chain: It is a useful platform designed for building and deploying dApps. Its mechanism is based on dual chain architecture consisting of BSC that deals with smart contract and dApps and Binance chain for handling the trading. It is compatible with Ethereum virtual machine enabling dApps built upon Ethereum network can be ported to BSC. It can communicate with other blockchains through Binance bridge [33].

l. Avalanche: To develop dapps and custom virtual machines, this interoperable open-source platform has been designed. It uses avalanche consensus algorithm for the selection of validators [34].

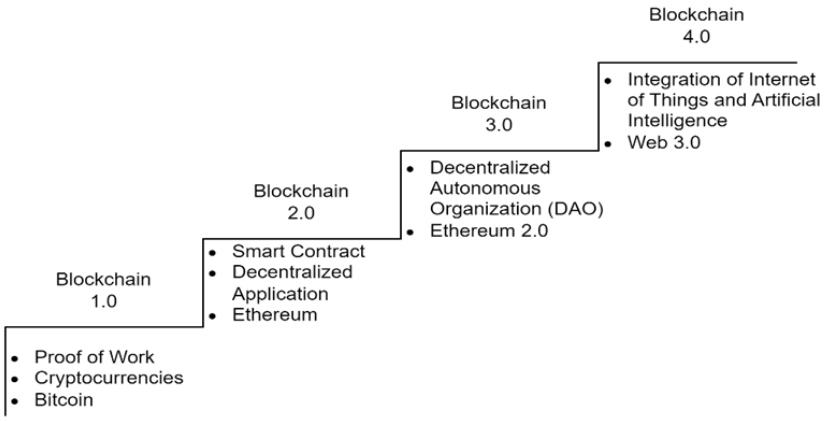

Fig. 1 Evaluation of Blockchain Technology

III. ARCHITECTURE OF BLOCKCHAIN

This section illustrates the General architecture of Blockchain that has five components such as Decentralized network, Distributed Ledger, and Cryptography, Structure of Block which depicted in Figure 2 and Consensus Mechanism.

a. Decentralized network: The underlying technology behind the blockchain is dependent upon P2P network, a type of decentralized network. In this network, each node has equal privileges as a result no central authority is needed for processing of data and not effected by a single point of failure.

b. Distributed Ledger: In Blockchain, this is a replicated data structure that is synchronized and replicated at every node across the network. It can be used to store transactions, smart contracts, Assets and digital identity.

c. Cryptography: It is a way of secret writing to achieve security features such as Data Integrity, Confidentiality, Non-repudiation, and Authentication. Cryptography techniques include Hashing, Encoding and Data encryption and decryption techniques. Blockchain makes the use of these techniques to protect its data from malicious attacks and modification.

A. Structure of Block in Blockchain 1.0

Finally, the structure of Block in Blockchain 1.0 comprises of a Block Header and a body part which includes all the transactions initiated on Blockchain. Block header consists of various fields including the hash value of previously added block, number only once (Nonce), Version, Merkle Root, difficulty bits (Nakamoto, 2008). The details are depicted below:

a. Hash value of Previous Block: If a block is not a Genesis block, it contains a hash value of previously added block in the blockchain. This hash value serves as a unique code for identifying the previously added block. A starting block in a Blockchain is known as a Genesis block. It does not refer to a previous block and was created by the network's founder.

b. Nonce: The nonce used in the mining of Bitcoin is a 32-bit arbitrary integer inserted to the block header to create a hash satisfying the target difficulty level. Miners seek for the proper nonce value using a brute force method in a such a way that the hash with given number of leading zeros results. The miner who discovers the proper nonce gets transaction fees and recently minted bitcoins and their block is entered onto the blockchain.

c. Merkle Root: In context of Bitcoin, it is a tree-based approach for generating a single hash value by combining the multiple transactions of a block through a bottom-up approach. The Merkle Tree operates by repeatedly hashing couples of transactions unless a singular hash value, referred to as the root hash, is found. The bottom layer of the tree contains the individual transaction hashes, and each subsequent layer above it has the hash of the prior layer's hashes, until the root hash is obtained. This enables the efficient and secure verification of the integrity of the transactions contained within a block. Figure 1 depicts this.

d. Time stamp: In Bitcoin, it represents an instant in time when a transaction or block was created or added to the Blockchain, and it is represented as number of seconds elapsed since January 1, 1970, midnight. By adding a timestamp to each transaction, the blockchain can establish the order in which transactions occurred, making it impossible for the same cryptocurrency to be spent twice.

e. Difficulty bits: For the block to be appended to the blockchain, the miner must determine the nonce. The level of difficulty involved in finding the nonce is not constant but depends on the difficulty bits. In Bitcoin mining, new transactions go through verification process and incorporated into the blockchain. Miners use specialized tools to solve a difficult math problem and create a unique code called a hash. The difficulty bits determine the minimum number of zeros that must be available at the beginning of a hash in order to add an additional block to the blockchain. The difficulty bits are adjusted by the Bitcoin network to keep the rate of block creation consistent. Higher difficulty bits mean it is harder to mine a block, while lower difficulty bits mean it is easier.

f. Version: It represents the current version of Bitcoin protocol being used for validating and creating the block.

g. Block Height: It shows where the block fits in the Blockchain. The Blockchain's first block, or genesis block, has 0 height and subsequent blocks have value one more than past block.

h. Size: It represents the size of the blocks in bytes.

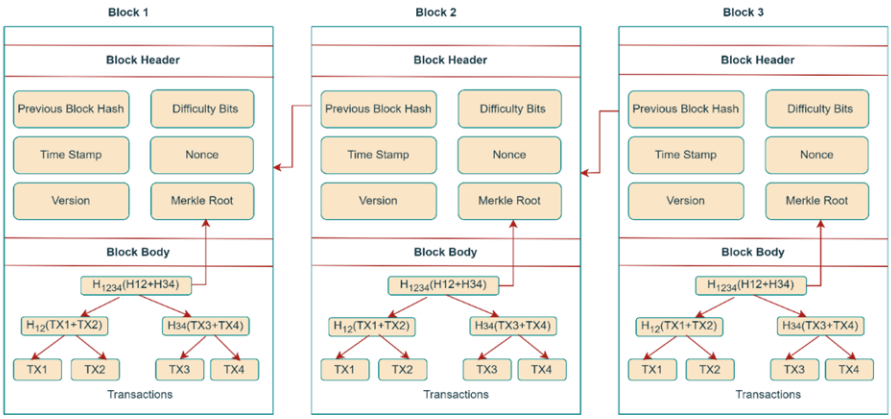

Fig. 2 Structure of Block in Blockchain

i. Block Reward: It is a reward given to a miner when a miner's block is successfully added to the blockchain. The network mints fresh bitcoin once a new block is built. This newly minted coin is given as a reward to the miner as well transaction fees of all transactions that are included in block.

j. Mining Fee: When a transaction that is a part of a longer chain is included in the Block, a miner gets paid a transaction fee.

IV. CONSENSUS MECHANISM

Prior to adding the block to the blockchain, every node in the distributed environment must agree upon a state of Blockchain. Various consensus algorithms that work on synchronous and asynchronous environments have been proposed for ensuring Consistency, Safety, Liveness, Integrity, Validity. Consensus algorithms distribute decision making power among participants rather than giving it to centralized authority. Various consensus algorithms are depicted below, and their comparison is depicted in Table 1.

1. Proof of Work (PoW): Basic principle of this algorithm relies on solving the cryptographic hash function in the form of hash puzzle. A miner, with the objective of incorporating an additional block into the blockchain, discovers the nonce that generates a hash with a specific preceding zero. To find the nonce, miners use high computing resources leading to wastage of electricity power. In each round, a miner who solves the puzzle first will be validated by the participants and other miners across the blockchain system. A Block is mined at regular interval of 10 minutes, and it will be considered if it is a part of longest chain [35].

2. Proof of Stake (PoS): To address the challenges of PoW, this algorithm relies on Percentage of total bitcoin a miner is holding. If the miner has 1% of the total amount of bitcoin in the network, they have 1% chance of adding the block to the blockchain. Here Miners are not using the high computing resources for solving the puzzle based on cryptographic function instead it relies on stake of Miners. More stakes mean more chance to add blocks to Blockchain and earn reward leading towards a centric approach. It starts after proof of work mined cryptocurrencies are evenly distributed in the network. It cannot work like a Bootstrapping Consensus mechanism. Another form of the PoS where participants have an opportunity to mine blocks on the blockchain depending on the number of days they had their coins is proof of coin age. Participants have more chances to add a block to the blockchain depending on how long they hold their coins [27].

3. Delegated Proof of Stake (DPoS): It is a PoS variant where Token holders vote to choose certain number of delegates also known as validators or Witnesses from a Pool of candidates [36] .

4. Proof of Authority (PoA): Validators are selected based on their established identity and reputation. These validators are typically individuals or organizations that are known and trusted within the network [37].They are granted the privilege for validating the transactions and Blocks. They are rewarded by cryptocurrency for their work like miners in PoW.

5. Proof of Burn (PoB): In this algorithm, miners need to provide proof to other participants across the network that they have burned the bitcoins by forwarding them to a verifiable address from where they cannot be accessible or sent again. This way miners can propose and validate new blocks and transactions. It also depends upon proof of work mined cryptocurrencies as we cannot start open blockchain network with it. First of all, we need to start with PoW then eventually we can move to PoB [38].

6. Proof of Elapsed Time (PoET): In this algorithm, every participant on the network awaits for a certain duration of time generated by the Trusted execution environment. A participant who awaits for a less period gets an opportunity to propose a new block. whether the participant has waited for a random period of a time or not, a special instruction called intel Software guard Extension is used [35]

7. Proof of Space: In this algorithm, A miner who has more drive space for storage gets a chance to mine the block rather than computation power. It is based on the creation of plots which are precomputed data structure.

These plots provide possible solutions to hash-based Puzzle. These miners generate plot consisting of nonce, timestamps, previous block hash values and transactions [39].

8. Paxos: In this Algorithms, there are three types of node roles such as proposer, acceptor, and learner. A node doesn't just have one job; it can do more than one thing, and there is a way for them to change things. There may

be one or more Proposers, whose job it is to make suggestions. There must be more than one acceptor. They vote on the proposal and either agree with it or not. If they don't agree, they reject it. The learner gathers the proposals that were agreed upon by all the acceptors and encourages the creation of the final proposal using the idea that the minority should follow the majority. The Paxos algorithm can be broken down into two main steps that are used in real life known as the preparation phase and the submission phase [40].

9. Raft: This algorithm is based on leader election and log replication mechanisms. It ensures cluster of servers agree on a sequence of log entries to be executed to make sure that all servers are in same state. Each node in the network can play the role of Leader, Follower and Candidate. The leader ensures the replication of log entries across all nodes, coordinating with other nodes and leader election. The follower responds to the AppendEntries RPCs, which contain information about log entries to be replicated, from the leader. These log entries are received from the leader. When followers effectively replicate log entries, they acknowledge the leader's action by responding to the AppendEntries RPCs. These responses serve to confirm that the entries have been securely received and stored in their own logs. When the current leader becomes unreachable due to failure, a leader election process starts by the Candidate. To start a leader election, a follower changes its role to candidate. A candidate must receive votes from a quorum defined as greater than half of all numbers of nodes in cluster to become the leader [41], [42].

10. Practical Byzantine Fault Tolerance (PBFT): It helps the different nodes in an asynchronous distributed environment agree on a certain thing, even if there are Byzantine faults. Byzantine faults refer to nodes behaving maliciously, arbitrarily, or experiencing other types of faults, and PBFT is designed to handle such scenarios while ensuring consensus. Raft and Paxos Algorithms have been designed to handle crash failure or Network partitioned but they don't handle Byzantine faults. PBFT offers guarantees in terms of safety, which ensures consensus on coherent values, and liveness, which maintains the system's forward momentum even in the presence of faults, provided that the count of faulty nodes remains within the threshold of one third of the total nodes. There are three roles that nodes can play in the PBFT network: Client, Primary (also called Leader), and Backup (also called Replica). The clients propose certain transactions in the form of request. The order of the request is purposed by the primary. When Backup receives the message, it verifies it and sends it to all the remaining nodes across the network. Each request progresses through Pre-Prepare, Prepare, and Commit phases. Initially a request is sent from the client to Primary. After getting the request from Client, Primary shares the pre-prepare message containing message type, timestamp, sequence no, digest of the request, signature, view no and node identifier information with backups. Backup receives the pre-pare message and validate its contents. Once the request is validated, Backup broadcasts the prepare message to all other nodes. Upon receiving Prepare messages from a minimum of 2f nodes, where f denotes the number of faulty nodes among other backup nodes and clients, the backup node broadcasts a Commit message. It then awaits the receipt of 2f Commit messages to achieve final consensus. If backups detect that the primary is faulty, a process is initiated to select a new primary by using round robin technique. This process is termed as View change [43].

Table 1 Comparison analysis of Consensus Algorithm [35], [37], [42], [44], [45], [46], [47], [48], [49]

Consensus Mechanism	Possible Attacks	Secure	Throughput (TPS)	Underlying Communication Method	Scalability	Suitable for Types of Blockchain	Block Creation Time	Fault Tolerance	Types of Faults Handled
Proof of Work (PoW)	51% attack	High	7 - 15	Broadcasting	Low	Public, Permissioned	Slow (10 - 120 minutes)	High	Node failures, network partitions
Proof of Stake (PoS)	Sybil attack	Medium	100 - 1000	Message Passing	Medium	Public, Permissioned	Medium (1 - 30 seconds)	Medium	Node failures, network partitions
Delegated Proof of Stake (DPoS)	Nothing-at-stake attack	Medium	1000 - 10000	Message Passing	High	Public, Permissioned	Fast (Less than 1 second)	High	Node failures, network partitions
Proof of Authority (PoA)	Collusion attack	Low	10000 - 100000	Message Passing	High	Permissioned	Fast (Less than 1 second)	High	Node failures, network partitions
Proof of Burn (PoB)	Double-spend attack	Medium	10 - 50	Message Passing	Low	Public, Permissioned	Slow (10 - 120 minutes)	Medium to High	Node failures,

									network partitions
Proof of Elapsed Time (PoET)	Spam attack	Medium	50 - 100	Broadcasting	Medium	Public, Permissioned	Medium (1 - 30 seconds)	Medium	Node failures, network partitions
Proof of Space	Denial-of-service attack	Medium	50 - 100	Broadcasting	Medium	Public, Permissioned	Medium (1 - 30 seconds)	Medium	Node failures, network partitions
Paxos	Message tampering attack	High	1000 - 10000	Message Passing	High	Public, Permissioned	Fast (Less than 1 second)	High	Byzantine faults, node failures, network partitions
Raft	Leader election attack	Medium	1000 - 10000	Message Passing	High	Public, Permissioned	Fast (Less than 1 second)	High	Byzantine faults, node failures, network partitions
PBFT	Partitioning attack	High	100 - 1000	Message Passing	Medium	Public, Permissioned	Medium (1 - 30 seconds)	High	Byzantine faults, node failures, network partitions
Bitcoin NG	Nothing-at-stake attack	Medium	100 - 1000	Broadcasting	Medium	Public, Permissioned	Medium (1 - 30 seconds)	Medium	Node failures, network partitions
Proof of Weight (PoW)	Sybil attack	Medium	10 - 50	Broadcasting	Low	Public, Permissioned	Slow (10 - 120 minutes)	Medium	Node failures, network partitions
Proof of Reputation (PoR)	Collusion attack	Medium	10 - 50	Message Passing	Low	Public, Permissioned	Slow (10 - 120 minutes)	Medium	Node failures, network partitions
Proof of History (PoH)	Message tampering attack	High	1000 - 10000	Broadcasting	High	Public, Permissioned	Fast (Less than 1 second)	High	Byzantine faults, node failures, network partitions

11. Bitcoin NG: It is an improved version of the Bitcoin Consensus protocol, with an aim to enhance the protocol's scalability and throughput. It achieves this by introducing key blocks and microblocks. Keyblocks play a role in leader election, while microblocks contain transactions. Like Bitcoin's blocks created at regular intervals

Table 2 Comparison analysis of various Frameworks/Platforms and Consensus Algorithm used by them [22], [23], [30], [50], [51], [52], [53], [54]

Platform	**Description**	**Consensus Mechanism**	**Main Programming Language**	**Smart Contracts Support**	**Governance Model**	**Privacy**	**Scalability**	**Inter-operability**	**Energy Efficiency**	**Security**	**Use Cases**
Bitcoin	Decentralized, immutable ledger of transactions	Proof of Work	C++	No	Community-driven	Low	Low	Low	Low	High	Digital currency
Ethereum	Decentralized, programmable blockchain	Proof of Work /Proof of Stake	Solidity	Yes	Decentralized	Low	Moderate	Low	Moderate	High	Smart contracts, decentralized applications
Polkadot	Interoperable blockchain platform	Nominated Proof-of-Stake	Various	Yes	Decentralized	Variable	High	High	Moderate	High	Interoperability between blockchains, cross-chain applications

Cardano	Third-generation blockchain with a focus on scalability, interoperability, and sustainability	Ouroboros Proof-of-Stake	Haskell, Plutus	Yes	Decentralized	High	High	High	High	High	Smart contracts, decentralized applications, governance
Solana	High-performance, low-cost blockchain	Proof-of-History	Rust	Yes	Decentralized	Variable	High	Moderate	High	High	High-throughput decentralized applications, DeFi
EOS	Decentralized, programmable blockchain	Delegated Proof-of-Stake	C++	Yes	Decentralized	Low	High	Moderate	Moderate	High	Smart contracts, decentralized applications
Ripple	Payment protocol for fast, low-cost transactions	Variant of Delegated Proof-of-Stake	C++	Yes	Centralized	Low	High	High	High	High	Cross-border payments, remittances
Binance Smart Chain	Smart contract platform built on Binance Chain	Proof-of-Staked Authority	Solidity	Yes	Centralized	Low	High	Low	Moderate	High	DeFi applications, NFTs
Tezos	Self-amending blockchain with on-chain governance	Liquid Proof-of-Stake	Michelson	Yes	Decentralized	High	Moderate	Low	High	High	Smart contracts, decentralized applications
Avalanche	High-performance, interoperable blockchain platform	Avalanche consensus	Solidity, C++	Yes	Decentralized	Variable	High	High	High	High	DeFi applications, cross-chain interoperability
Algorand	Pure proof-of-stake blockchain focused on scalability and security	Pure Proof-of-Stake	TEAL, PyTEAL	Yes	Decentralized	High	High	Low	High	High	Financial applications, asset tokenization
Hedera Hashgraph	Fast, secure, and fair distributed ledger technology	Hashgraph consensus	Java	Yes	Decentralized	Low	High	High	High	High	Supply chain tracking, digital identity
NEAR Protocol	Developer-friendly, high-throughput blockchain	Proof-of-Stake	Rust	Yes	Decentralized	High	High	High	High	High	Decentralized applications, DeFi
Corda	Designed for financial services	BFT	Java	Yes	Consortium	High	High	High	High	High	Trading, Know Your Customer (KYC), Digital Identity management
Hyperledger	Framework for enterprise blockchain	Pluggable Consensus Algorithm	Various	Yes	Community with individual framework	Vary	Vary	Vary	Vary	Vary	Enterprise Based Blockchain applications.

of 10 minutes through the standard mining process, keyblocks are also generated at regular 10-minute intervals. They contain the list of validators (i.e Miners) who have been elected to be leader in the next round. After a leader is chosen, it is granted an opportunity to generate microblocks at a much higher rate compared to keyblocks before the next leader is elected. These microblocks, bearing the leader's signature, are then disseminated across the network. Subsequently, miners validate and incorporate these microblocks into the blockchain [55].

12. Proof of Weight: It is based on the Algorand consensus model and adds the idea of "weight" to the basic idea of Proof of Work. [29]. Unlike single consensus algorithms such as PoW or PoS, it functions as a collection of consensus algorithms. The goal is to address the challenges present in them. The way it operates involves assigning a weight to each node in the network based on the contributions of the node. The number of tokens possessed by

the node is one of the factors that decide this weight. Node's reputation, the amount of storage space provided, or other criteria relevant to the purpose of the network. A higher weight gives a node a better chance of mining the next block to the Blockchain. A committee made up of randomly selected network members is formed by the network whenever a transaction takes place on a blockchain. This committee uses the Proof-of-Weight consensus process to determine each member's weight. By taking this technique, the committee's consensus-building process is somewhat centralized, which guarantees a secure and quick consensus across the network. Assigning a weight to each node prevents double spending attack, sybil attack in which attacker creates false identities to gain the control on the network and forking.

13. Proof of Reputation (POR): This is a more secure form of PoA that relies on the identity of the validator and verifies and validates the blocks and transactions by a group of trusted validators or authorities. In this, Blocks are added by those nodes which have a good reputation in the network. The reputation is based on consistent validation of transactions correctly, prompt response to a request or consistent availability. To keep the track of behavior and contribution of each node a reputation management system is used [48].

14. Proof of History (PoH): It is based on high frequency verifiable delay function that is used to generate a distinct output, which can be validated and verified publicly, but it requires a certain number of consecutive steps for evaluation process for adding a delay in decentralized application. It was first introduced by Solana Lab [27].

V. CONCLUSION

Blockchain frameworks and consensus algorithms are critical components of decentralized systems that provide a diverse array of applications in a variety of sectors including finance, healthcare, supply chain management, and voting systems. These technologies offer a secure, transparent, and immutable ledger for the processing of transactions and data management. Blockchain frameworks, including Hyperledger Fabric, Corda, and Ethereum, can be employed to offer solutions that range from public decentralized applications (dApps) to enterprise-grade solutions, each with its own distinctive features and capabilities. Consensus algorithms, including Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), offer a solution in the areas of security, efficiency, and scalability. This enables developers to utilize these algorithms in accordance with the requirements of their application.

ACKNOWLEDGMENT

The author would like to thank Prof. Ambarish Sharan Vidyarthi honorable vice chancellor of Bikaner Technical University, Bikaner and Dr S M Prasanna Kumar director B K Birla Institute of Engineering and Technology, Pilani for their continuous support and Guidance.

REFERENCES

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system, October 2008," *Cited on*, 2008.

[2] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System," *IEEE Access*, vol. 6, 2018, doi: 10.1109/ACCESS.2018.2870644.

[3] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer Peer Netw Appl*, vol. 14, no. 5, 2021, doi: 10.1007/s12083-021-01127-0.

[4] S. Y. Lin, L. Zhang, J. Li, L. li Ji, and Y. Sun, "A survey of application research based on blockchain smart contract," *Wireless Networks*, vol. 28, no. 2, 2022, doi: 10.1007/s11276-021-02874-x.

[5] S. K. Panda and S. C. Satapathy, "Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers," *Pers Ubiquitous Comput*, vol. 28, no. 1, 2024, doi: 10.1007/s00779-021-01588-3.

[6] A. Rejeb *et al.*, "Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions," 2024. doi: 10.1016/j.iotcps.2023.06.003.

[7] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *Journal of Cryptology*, vol. 3, no. 2, 1991, doi: 10.1007/BF00196791.

[8] R. C. Merkle, "Method of Providing Digital Signatures," 1982

[9] D. Chaum, "David Chaum: DigiCash CEO," *Forbes*, 1996.

[10] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2896108.

[11] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," 2021. doi: 10.1109/ACCESS.2021.3072849.

[12] F. Hashim, K. Shuaib, and N. Zaki, "Sharding for Scalable Blockchain Networks," 2023. doi: 10.1007/s42979-022-01435-z.

[13] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K. K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," 2020. doi: 10.1016/j.jnca.2019.102471.

[14] L. D. Negka and G. P. Spathoulas, "Blockchain State Channels: A State of the Art," *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3131419.

[15] N. Papadis and L. Tassiulas, "Blockchain-Based Payment Channel Networks: Challenges and Recent Advances," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3046020.

[16] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," 2022. doi: 10.1145/3471140.

[17] S. Peng *et al.*, "Blockchain Data Secure Transmission Method Based on Homomorphic Encryption," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/3406228.

[18] M. Dieye *et al.*, "A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain," *IEEE Access*, vol. 11, 2023, doi: 10.1109/ACCESS.2023.3268768.

[19] P. W. Chi, Y. H. Lu, and A. Guan, "A Privacy-Preserving Zero-Knowledge Proof for Blockchain," *IEEE Access*, vol. 11, 2023, doi: 10.1109/ACCESS.2023.3302691.

[20] L. Liu, S. Zhou, H. Huang, and Z. Zheng, "From Technology to Society: An Overview of Blockchain-Based DAO," *IEEE Open Journal of the Computer Society*, vol. 2, 2021, doi: 10.1109/OJCS.2021.3072661.

[21] V. Buterin, "Ethereum White Paper," *Etherum*, no. January, 2014.

[22] S. Barac, I. Boticki, G. Perkovic, V. Radosevic, and I. Terzic, "Cardano - What Is It and How to Start Working with It," in *2023 46th ICT and Electronics Convention, MIPRO 2023 - Proceedings*, 2023. doi: 10.23919/MIPRO57284.2023.10159944.

[23] H. Abbas, M. Caprolu, and R. Di Pietro, "Analysis of Polkadot: Architecture, Internals, and Contradictions," in *Proceedings - 2022 IEEE International Conference on Blockchain, Blockchain 2022*, 2022. doi: 10.1109/Blockchain55522.2022.00019.

[24] T. N. Dinh and M. T. Thai, "AI and Blockchain: A Disruptive Integration," *Computer (Long Beach Calif)*, vol. 51, no. 9, 2018, doi: 10.1109/MC.2018.3620971.

[25] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," 2016. doi: 10.1109/ACCESS.2016.2566339.

[26] J. R. Jensen, V. von Wachter, and O. Ross, "An Introduction to Decentralized Finance (DeFi)," *Complex Systems Informatics and Modeling Quarterly*, vol. 2021, no. 26, 2021, doi: 10.7250/csimq.2021-26.03.

[27] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2925010.

[28] L. Baird, M. Harmon, and P. Madsen, "Hedera A Governing Council & Public Hashgraph Network," *White Paper*, no. 1.2, 2018.

[29] J. Chen and S. Micali, "Algorand: A secure and efficient distributed ledger," *Theor Comput Sci*, vol. 777, 2019, doi: 10.1016/j.tcs.2019.02.001.

[30] A. Yakovenko, *Solana: A new architecture for a high performance blockchain v0.8.13*. 2019.

[31] W. Song *et al.*, "EOS.IO blockchain data analysis," *Journal of Supercomputing*, vol. 78, no. 4, 2022, doi: 10.1007/s11227-021-04090-y.

[32] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm," Jul. 2018. [Online]. Available: https://ripple.com/files/ripple_consensus_whitepaper.pdf

[33] "Binance Smart Chain White Paper," Jul. 2022. [Online]. Available: https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md

[34] D. Tanana, "Avalanche blockchain protocol for distributed computing security," in *2019 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2019*, 2019. doi: 10.1109/BlackSeaCom.2019.8812863.

[35] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, "On the security and performance of Proof of Work blockchains," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2016. doi: 10.1145/2976749.2978341.

[36] D. Larimer, "DPOS Consensus Algorithm - The Missing White Paper," *URL: https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper*, vol. 2018, 2017.

[37] Md. M. Islam, M. M. Merlec, and H. P. In, "A Comparative Analysis of Proof-of-Authority Consensus Algorithms: Aura vs Clique," in *2022 IEEE International Conference on Services Computing (SCC)*, 2022, pp. 327–332. doi: 10.1109/SCC55611.2022.00054.

[38] K. Karantias, A. Kiayias, and D. Zindros, "Proof-of-Burn," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020. doi: 10.1007/978-3-030-51280-4_28.

[39] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015. doi: 10.1007/978-3-662-48000-7_29.
[40] L. Lamport, "Paxos Made Simple," 2001.
[41] J. Hu and K. Liu, "Raft consensus mechanism and the applications," in *Journal of Physics: Conference Series*, 2020. doi: 10.1088/1742-6596/1544/1/012079.
[42] D. Huang, X. Ma, and S. Zhang, "Performance Analysis of the Raft Consensus Algorithm for Private Blockchains," *IEEE Trans Syst Man Cybern Syst*, vol. 50, no. 1, 2020, doi: 10.1109/TSMC.2019.2895471.
[43] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," 1999.
[44] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017. doi: 10.1007/978-3-319-69084-1_19.
[45] B. Cao *et al.*, "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, 2020, doi: 10.1016/j.dcan.2019.12.001.
[46] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, 2020, doi: 10.1016/j.future.2017.08.020.
[47] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications*, vol. 3, no. 2, 2022, doi: 10.1016/j.bcra.2022.100067.
[48] Q. Zhuang, Y. Liu, L. Chen, and Z. Ai, "Proof of reputation: A reputation-based consensus protocol for blockchain based systems," in *ACM International Conference Proceeding Series*, 2019. doi: 10.1145/3343147.3343169.
[49] Y. Alabdulkarim, A. Alameer, M. Almukaynizi, N. Allheeib, F. Alkadyan, and A. Almaslukh, "Managing Expatriate Employment Contracts with Blockchain," *Electronics (Switzerland)*, vol. 12, no. 7, 2023, doi: 10.3390/electronics12071673.
[50] M. Conti, K. E. Sandeep, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4, 2018, doi: 10.1109/COMST.2018.2842460.
[51] I. Amores-Sesar, C. Cachin, and J. Micic, "Security Analysis of Ripple Consensus," in *Leibniz International Proceedings in Informatics, LIPIcs*, 2021. doi: 10.4230/LIPIcs.OPODIS.2020.10.
[52] M. Benji and M. Sindhu, "A study on the Corda and Ripple blockchain platforms," in *Advances in Intelligent Systems and Computing*, 2019. doi: 10.1007/978-981-13-1882-5_16.
[53] L. Goodman, "Tezos -a self-amending crypto-ledger White paper," 2014. [Online]. Available: https://tezos.com/whitepaper.pdf
[54] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, 2018. doi: 10.1145/3190508.3190538.
[55] I. Eyal and E. G. Sirer, "Bitcoin-NG: A Secure, Faster, Better Blockchain," *J Chem Inf Model*, 2015.