International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I5P204

Volume 71 Issue 5, 27-39, May 2023


*Review Article*

# Blockchain Technology Review : Consensus Mechanisms and Applications

Mahantesh N. Birje[1], R. H. Goudar[2], C. M. Rakshitha[3], Manisha T. Tapale[4]

[1,2,3]*Department of CSE, Visvesvaraya Technological University, Belagavi, India.*
[4]*Department of CSE, KLE MSSCET, KLE Technological University Belagavi, India*.

[3]*Corresponding Author : rakshithacm3@gmail.com*

Received: 13 February 2023 Revised: 15 April 2023 Accepted: 06 May 2023 Published: 25 May 2023

***Abstract*** *- Blockchain technology is currently gaining a lot of attention from industry and academia due to its notable and distinctive features. From a monetary standpoint, the technology was initially disregarded because it was seen as nothing more than a cryptocurrency(money) community network. But it now promises to upgrade existing models in almost all sectors, including not only information technology and business but also e-community sectors such as government, media, medicine, law, and supply chain management (SCM). The approach, also known as Distributed Ledger Technology (DLT), makes data immutable and visible using cryptographic hashing. Decentralized trust through consensus algorithms is an important and vital feature of technology that contributes to its widespread adoption. Consensus algorithms also help the network achieve Consistency, Availability, and Partition tolerance all at the same time, but traditional distributed technology encounters a conflict in doing so. This study investigated blockchain basics, such as essential features, blockchain network types, and distinct application domains, with a focus on a taxonomy of consensus mechanisms. A thorough survey of approximately 60 papers was undertaken to comprehend the key ideas underlying blockchain technology. This review paper supports scholars in knowing researching the fundamentals of blockchain technology and its potential applications.*

***Keywords*** *- Blockchain, Consensus mechanism, Distributed Ledger Technology, Taxonomy, Trust.*

## 1. Introduction

The uniqueness and widespread acceptance of blockchain technology can be attributed to the manner it is presented as well as the benefits it provides. An immutable, public, or transparent ledger of transactions is synchronized across all nodes in the distributed ledger in real-time. Blockchain extends far beyond the realm of bitcoin and digital wallets. There is no debate about the importance of bitcoin to the functioning of blockchain [1], but the technology's applications go far beyond the financial sector[2,5]. Information is relayed between terminals using an unprotected broadcast method in today's digital world. [2].

Privacy, which includes confidentiality, is a top priority in this context. In the current digital environment, encrypted peer-to-peer messaging using Blockchain technology that does not rely on a network's central controller can be seriously examined. Anybody with access to the internet can view these transactions, yet no one has ever been able to alter any of the information contained therein. Unlike traditional databases, which are typically stored in trusted centralized locations like banks and national government statutes, blockchain is not owned by any one entity. The technique guarantees immutability; thus, information can never be altered. Anonymity – the use of hash functions to protect the privacy of users. Consensus algorithms, or an algorithm for reaching consensus, Contracts that be executed using a digital platform and are predicated on a preexisting agreement are known as smart contracts. Its faster transactions and higher security features have earned it widespread recognition and trust. Despite these advancements and various advantages, some sensitive concerns still need to be addressed, such as making the new system scalable and adaptable and outlining the possible regulation rules in Distributed ledger Technology, which can be seen as limitations.

The CAP Theorem states that it is impossible for distributed systems to achieve consistency, availability, and partition tolerance simultaneously; it is also regarded as a huge disadvantage. Consistency- At that point in time, each node contains the same type of data., Availability- It is calculated as a percentage of network active time and Partition Tolerance- It can be described as how well a network will tolerate and work with malicious nodes. All of these elements are handled by blockchain via the consensus method. So the goal of this article is to delve deeper into the consensus mechanism and other principles that make blockchain technology immune to all network difficulties.

This paper will follow the outline below.

In section 2, Fundamentals of Blockchain Technology has been provided in a graphical format where the main principles of the technology have been explained in a more systematic and organised manner to assist future scholars in gaining an understanding of crucial components.

Subsection 2 outlines the basic features, types, and consensus methods of blockchain and briefly explains the classification of its application in various domains.

Section 3 provides a summary of this research article.

## 2. Fundamentals of Blockchain

Blockchain technology's innovative and consequential nature can be traced back to a few key concepts. Taxonomy, comparison tables, and other methods were employed to organize the fundamentals of this research further. The principles of Blockchain technology are depicted in Figure 1.

### *2.1. Key Features*

Some of the most noteworthy features of blockchain are covered below:

#### *2.1.1. Decentralized Technology and Consensus Mechanism*

By removing the requirement for a central authority or reliable third party to oversee the entire system, decentralization gives the blockchain more power. Decentralization is propelled by the consensus process. Each node in the blockchain network will employ a consensus method to reach an agreement on a shared set of rules. A consensus layer has been built into the architecture of this system to control and decide upon crucial aspects of the system [4].

In the next section, we go deep into the consensus mechanism. When using the consensus method, concerns about the reliability of technological systems are eliminated[11]. One of the most crucial reasons, alongside trust, that a network would opt for decentralization is that it is adept at Fault-Tolerance in a peer-to-peer grid. Any distributed system will likely favor the decentralized system due to its immunity to a single-point failure. Bitcoin and Ethereum, two digital currencies, make extensive use of decentralized systems.

#### *2.1.2. Distributed Ledger Technology(DLT)*

All network nodes store the same data simultaneously, clearly defining DLT [5]. Each computer in the network has its own copy of the digital ledger, which they must check as the transaction progresses. Although blockchains and distributed ledgers share many similarities, not every distributed ledger is a blockchain. The primary difference between a blockchain and a distributed ledger is that the latter does not use blocks to keep the ledger growing. One example that facilitates differentiation is R3's corda.

The cryptocurrencies Ethereum and Bitcoin are two instances of blockchain technology [4]. In recent years, "Blockchain" has become a widely accepted acronym for "Distributed Ledger Technology" or "DLT".

#### *2.1.3. Smart Contracts*

When nodes agree to have transactions with adequate consensus, they are written programs that execute on the topmost layer of the blockchain [7]. They automate independent treaty execution with no middleman or time lag. Every participant is regularly assured of their choice. The smart contract logic may cause transaction results or outcomes to change. Miners are the ones who write the code for the smart contract in their preferred language, such as java or Python.

In this case, the name is smart, but the contract accomplishes exactly what it is supposed to do. In blockchain technology, this deterministic quality of smart contracts is desired when it consistently generates the same outcome based on the program. An exact compiler can be used to turn the code into a bytecode to establish a logical contract [15].

#### *2.1.4. Immutability and Enhanced Security*

Because of its capacity to remain unchanged or unaltered, immutability is typically considered the technology's defining characteristic. Numerous hash functions, digital signatures, public key cryptography, and Merkle tree patterns make it the most secure cryptographic algorithm currently available. There are numerous instances outside of banking in which data integrity must be maintained. In the cloud sector, platforms, data, and software are in the public domain [36]. Numerous industries have adapted cloud computing; however, security verification is essential in this type of environment [62], and data can be exposed rapidly if a malicious user is present in the system. Confidential government initiatives can be compromised with relative ease if there are flaws in the information security system [14].

In this regard, data integrity must never be compromised. DLT encourages transparency while making it resistant to malfeasance. For instance, if an intruder or malicious operator wishes to alter prior Bitcoin blocks, Proof of Work (PoW) must be replicated for each and every prior block contributed to the blockchain, thereby making the method more complicated and the blockchain immutable [16].

### *2.2. Types of Blockchain Network*

Blockchain technology was declared a Public Type with a cryptocurrency use case when it was first utilized [1]. With time, its uses have expanded and are not limited to bitcoin. In some circumstances, a public network is not the ideal option for an application. Based on how it is now used in various contexts, the blockchain network has been segmented into three distinct categories.

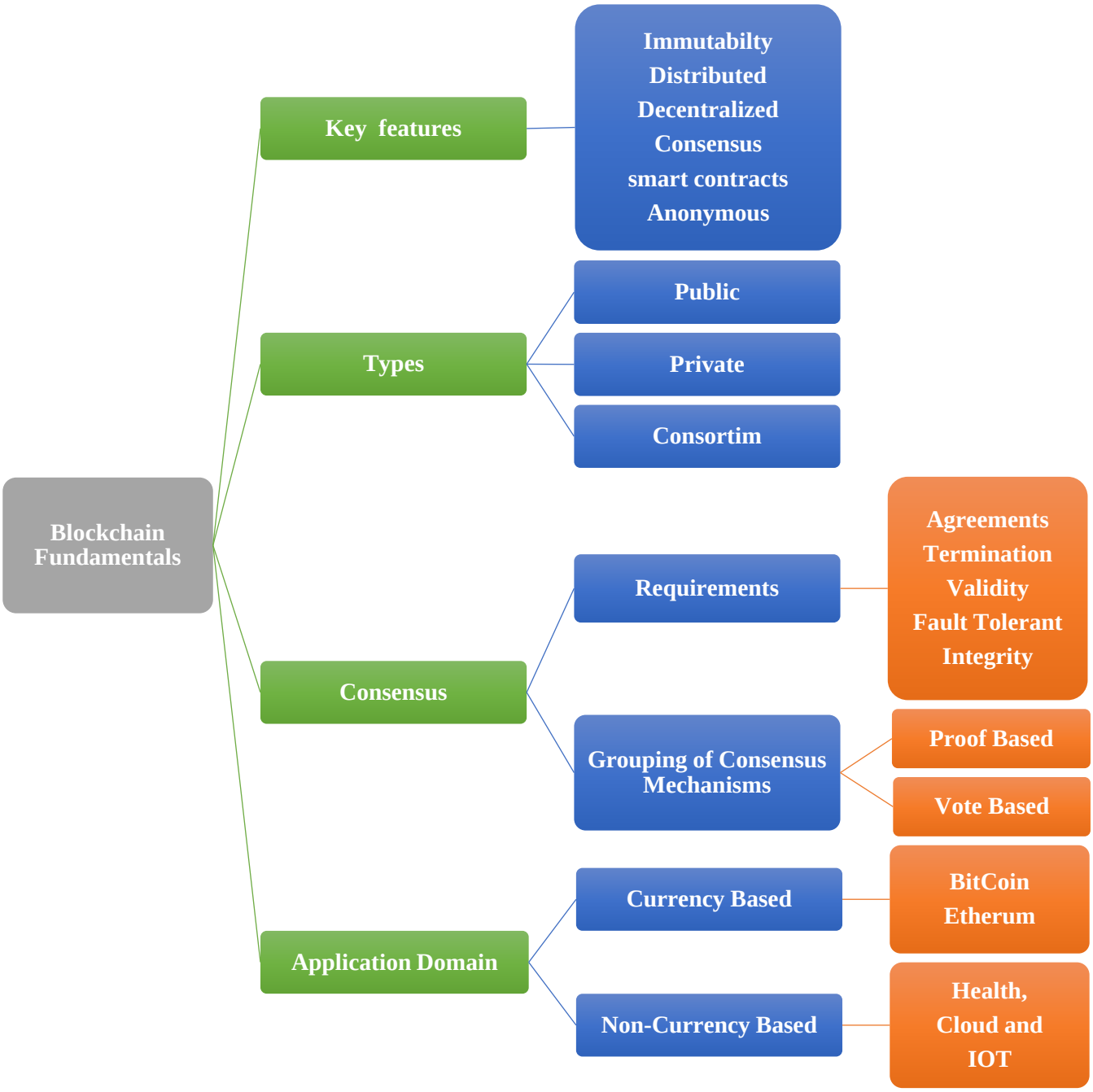


**Fig. 1 Key aspects of blockchain technology**

*2.2.1. Public Blockchain*

The public blockchain is totally decentralized and not controlled by any one entity. The term "public" suggests that no one will have exclusive access to information but rather that it would be made available to everybody for input during the decision-making process [4].

Since the network is open to the public, creating new blocks is a computationally intensive process that results in high transaction fees. In public or permissionless ledgers, users keep a copy of the ledger on their local nodes and use a distributed consensus process to determine the final state of the ledger, regardless of whether or not they are compensated for their participation. Therefore, all public network nodes are of equal significance.

*2.2.2. Private Blockchain*

These blockchains continue to maintain their order and confidentiality [5], as their names imply. Private blockchains, in contrast to public blockchains, operate based on

permissions, and each node in the network may be an officially acknowledged member of a single organization.

*2.2.3 Consortium Blockchain*

These blockchains are similar to private blockchains used by organizations with exclusive access to the internet. It maintains openness among all parties involved while incorporating several levels of authority into the network [7]. Data transfers between consortium members are recorded, and block creation and publication are computationally low-priced. Since it may not always be necessary to use complex consensus algorithms, it is not truly decentralized. Finally, this blockchain kind is common in institutions where a number of separate entities must work together, such as banks. Three distinct blockchains and the use cases they best suit are compared in Table 1.

### *2.3. Consensus Mechanism*

Consensus is an essential component of blockchain technology and a central pillar of the technology. It is a treaty mechanism between n nodes in a distributed network, which is the defining characteristic for tusting the technology. In distributed technologies, where multiple nodes contribute to transactions and a blockchain network develops in accordance with various consensus algorithms, the agreement is a difficult challenge. Although computer scientists and academics have studied a digital agreement mechanism for many years, its prominence grew with the advent of blockchain, bitcoin, and the Proof of Work (PoW) algorithm. Certain prerequisites must be met for a consensus mechanism to yield the desired outcome. Several of these essential requirements include the following:

*2.3.1. Agreement*

Authentic nodes have total control over the same value.

*2.3.2. Termination*

When all of the authentic nodes in the network have come to a conclusion, the execution of the consensus progression will be complete.

*2.3.3. Validity*

It is necessary for the value that all genuine nodes have come to a consensus on to be identical to the value provided initially by at least one legitimate node.

*2.3.4. Fault-Tolerant*

The consensus technique should continue to function normally even when there are broken or malicious nodes (also known as Byzantine nodes).

*2.3.5. Integrity*

It is essential that within the course of a single consensus cycle, not a single node is able to reach the same conclusion more than once.

*2.3.6. Types of Consensus Mechanisms*

Consensus processes are developed completely to take on n commitments in the distributed system and allow the arrangements to succeed in a final agreement state. These consensus methods can be categorized into two major groups. These groups can deal with practically any problem that may arise in a decentralized system. As shown in Fig. 2, the Taxonomy of Consensus Mechanism provides a detailed look at the various levels of categorization and subdivision that make up these groups.

- Vote Based
- Proof-based/Leader election

*2.3.7. Vote Based*

This democratic approach to reaching consensus is alluded to by the phrase "vote based," which describes how the process works. It does this by tallying the votes cast by the nodes that make up the peer-to-peer network. This leads to the achievement of transactional consensus. This can be further broken down into two distinct categories.

- Byzantine Fault Tolerance
- Crash Fault Tolerance

Traditional Byzantine Fault Tolerance (BFT)-based: Because it utilizes an enormous number of different hash functions, it is not entirely computation-based. The pact is considered established once a predetermined minimum number of communications have been acknowledged [22]. This is an older method that has garnered a great deal of support throughout the years [4]. The following are the two necessary protocols that are specified here:

- Practical Byzantine Fault Tolerance(PBFT)
- Federated Byzantine Agreement

**Table 1. Comparison of blockchain types**

| Types | Application Scenarios | Participation in consensus | Immutability | Transaction processing speed |
|---|---|---|---|---|
| **Public** | Bitcoin and Ethereum | All nodes | Impossible to tamper | Slow |
| **Private** | Hydrachain and Quorum | Single organization | Could be tampered | Fast |
| **Consortium** | R3, Corda | Choose n nodes in organizations | Could be tampered | Fast |

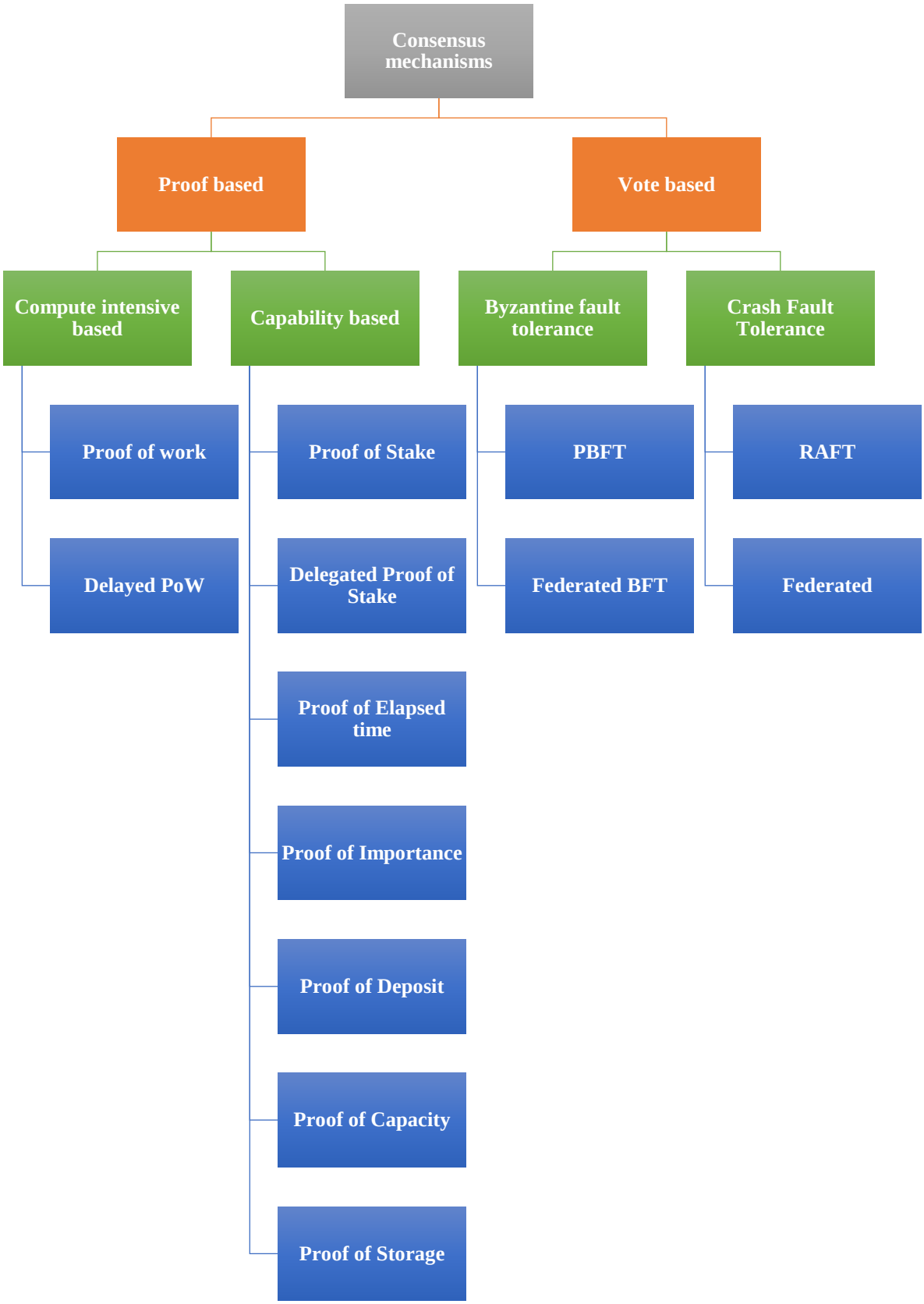


**Fig. 2 Taxonomy of consensus mechanism**

*2.3.8. Crash Fault Tolerance Based*

Even though one of the node's components has stopped working and the node itself is worn down, the algorithm will still successfully complete the task. Through the use of this method, tolerance and agreement are fostered. The following are the two most crucial procedures:

- RAFT
- Federated

*2.3.9. Proof Based*

Proof of effort, computational control, or other important aspects must be shown consistently for this strategy to create consensus. The procedure necessitates competitive bidding between nodes, with the preferred node submitting the winning bid. As an example, Bitcoin's proof-of-work system may now be explained. The following two groups, which are proof-based, are further divided into:

- Compute intensive based
- Capacity based

*a) Compute Intensive Based*

The leader will be chosen based on their performance in this procedure. The hash computational function is important; whoever calculates this mechanism profligately and proficiently with all of the necessary resources will be elected as a leader. The following algorithms are derived from this categorization.

*b) Proof of Work (PoW)*

PoW is the most commonly utilised in public networks. For example, bitcoin and litecoin. It only works based on the efficient use of processing resources and the ability to solve difficult computations [19]. It must be adept at solving mathematical riddles as well as performing hash computations. PoW has proven to be one of the most common and effective algorithms for dealing with collisions on a blockchain network, such as the Sybil attack.

*c) Delayed PoW*

PoW is a compute exhaustive protocol but an energy-starving protocol. Delayed PoW follows energy-efficient or capability-designed protocols that employ the compute exhaustive feature of PoW to protect various blockchain networks. As a result, the Delayed PoW method is also referred to as a hybrid consensus approach. [21].

*d) Capability-Based*

The leader will be chosen based on a miner's expertise, i.e. cryptocurrency that the miner specifically owns. Sideways with the amount of currency, the miner's role in the business contract network, the network's trust, or the amount of storage maintained by the miner. This is where the subsequent algorithms come from.

*e) Proof of Stake (PoS)*

This algorithm is based on a node's or user's stake fraction. If the miner has a large enough stake in the system, any malevolent effort from that handler will outweigh the benefits of a network assault. Peer Coin announced and supported this approach from the beginning.

*f) Proof of Elapsed Time(PoET)*

This technique was released by Intel in 2016. The critical features of randomness and security inside the development are guaranteed by Trusted ExecutionEnvironment(TEE) via promised wait time. Every member of the blockchain network waits for an unpredictable length of time. The leader of the new block is the first person to complete it. Attestation and the Trusted Execution Environment(TEE) are used to confirm that the proposer has indeed waited.

*g) Proof of Deposit (PoD)*

In this case, a security deposit must be made by the contributing nodes before they can begin mining. This security deposit is used as proof. The Tendermint blockchain has approved this technique.

*h) Proof of Capacity (PoC)*

In this layout, the hard disc storage edge is defined as the capability to mine the blocks. Hard drive mining is an alternative name for it. PoC differs from PoW in that the latter considers CPU resources.

*i) Proof of Storage (PoS)*

This plan is based on the available storage space and permits outsourcing of storage capacity.

*j) Proof of Importance (PoI)*

It, too, interprets how much stake the user has given, but the concept is crucial, which differs from Proof of Stake. Whereas the latter is based on the size of the user's investment, PoI also tracks token movement through the user to determine the level of reliance and relevance. The three consensus algorithms used by the majority of blockchain applications today are PoW, PoS, and PBFT. Table 2 compares three consensus methods, which include both proof-based and vote-based techniques. It quantifies time, space, and other critical qualities.:

*2.3.10. Decentralized Trust through Consensus Mechanisms*

Many studies have demonstrated [41] that they must rely on trust procedures and third parties or intermediaries in centralised contexts to ensure data integrity. There is no need for any trustworthy third parties with blockchain technology because the technology itself assures confidence. Its key quality is immutability, which allows the data to be trusted by the technology. Every technical aspect, such as creating a new block or verifying data, must go through consensus procedures and smart contracts, which give each node in the network equal power and make it decentralised. Table 3 provides a summary of several scientific contributions in the field of decentralised trust.

**Table 2. Comparison of consensus mechanisms**

| Consensus algorithms | | | |
|---|---|---|---|
| | Proof based | | Vote based |
| | PoW | PoS | PBFT |
| **Verification speed** | Slow | Normal | Fast |
| **Energy consumption** | Very high | Normal | Low |
| **Degree of Centralization** | Very low | Normal | High |
| **Security** | Secure | Secure | Least Secure |
| **Transaction finality** | Probabilistic | Probabilistic | Immediate |
| **Token needed** | Yes | Yes | No |
| **Network scale** | Large | Small | Small |
| **Nodes for identity management** | without approval | without approval | without approval |
| **Example** | Bitcoin | Ethereum | Hyperledger |

**Table 3. Brief details of decentralized trust achieved from various researches**

| Various research articles | Main feature | Decentralized trust ensured from |
|---|---|---|
| **[52]** | Unswerving data storage, supervising and verification, integrity protection | The unique hash value that complies with the file is produced by the Merkel hash tree, consensus, and blockchain smart contracts. |
| **[53]** | Origin information can be used to establish the integrity of outsourced data. | Blockchain technology with consensus and smart contracts. |
| **[54]** | A method for decentralised storage that is effective for testing data integrity | construction of an arbitration method, consensus, and smart contract as a sampling approach. |
| **[55]** | In a smart city, there is an access control system called (Subject-Object-Task System). | Access control regulations are included in the consensus and smart contracts of blockchain. |
| **[56]** | making sure that the commerce ecosystem is secure and trustworthy. | DLT and smart contracts followed by consensus make it a trusted decentralized system. |
| **[57]** | It offers a great level of trust, transparency, and security | Consensus and Ethereum Smart contracts. |

### *2.4. Application Domains*

Blockchain technology vastly improves upon several existing cryptographic security methods[27]. In addition to digital currencies like Bitcoin and Ethereum, it can be used in the fields of medicine, education, the internet of things (IoT), and even agriculture. The paper's application scenarios are divided into two categories: those that involve currency and those that do not, to help readers grasp blockchain's significance in both monetary and non-monetary contexts.

#### *2.4.1. Non-Currency Based*

In this article, some of the core uses of blockchain technology, such as pharma supply chain management (SCM) in the healthcare industry and the Internet of Things, have been explored. Blockchain technology enables a wide range of non-currency applications.

*Health Care and Medical Supply Chain*

The healthcare business can benefit from blockchain technology in a number of ways, such as the safe transfer of patients' medical records, the completion of the medicine supply chain, and the aid of healthcare researchers. These are but a few of the many potential uses in the medical field. [29]. Careful management of the drug supply chain is of paramount importance. Undoubtedly, the world is witnessing such an event right now, as the covid-19 pandemic has given rise to numerous worries. Because of the sensitive nature of the pharmaceutical goods being transported from one site to another, the healthcare industry relies significantly on the pharmaceutical supply chain. Due to the high demand for drugs and vaccines within the healthcare SCM, supply chain management (SCM) is a challenging undertaking, since dishonest users continuously strive to disrupt the supply chain and mislead the entire network for their own illegal benefits.

The pharmaceutical supply chain includes pharmaceutical companies, healthcare facilities, wholesalers, and retailers. Blockchain technology can be used to organize better supply chain management, an essential concept for efficiently distributing medicines, emergency supplies, and vaccination. Prescription fraud, ineffective pharmaceutical use, and a lack of an unbreakable audit trail necessitate state-of-the-art technology for these stakeholders. A new use case for blockchain technology in the pharmaceutical supply chain has been proposed [58]. Without a doubt, Blockchain Technology has attracted more focus in this area as a reliable and secure network[52][58][59].

Important traits like decentralization, persistence, immutability, anonymity, and auditability could protect medication and vaccine supply chains from attacks by vindictive users[31].

Blockchain benefits or services for the pharmaceutical industry include:

- Persistent pharmaceutical product tracing.
- Losses from counterfeiting were reduced.
- Transparency will increase accountability.
- Efficient and effective recall management.

*Internet of Things*

Blockchain technology has the potential to be implemented in a variety of Internet of Things use cases in order to streamline and strengthen the network's security [39,40,42]. The Integration scheme and Trustless architecture of the Internet of Things have been illustrated in this section.

*Blockchain and IoT's Integration Schemes*

During the development of the Internet of Things, centralized cloud services have played an important role. The only cause for concern with regard to that kind of service is a lack of faith in the information's transparency, mainly due to the fact that users of IoT don't have control over information sharing nor complete faith in it. In addition, these centralized cloud services are vulnerable to a wide variety of different kinds of errors and assaults.

When compared to Fog and Mist architecture [40], the evolution of the Internet of Things improves the supplementary functions at the network edge. With the deployment of blockchain technology, concerns regarding the trustworthiness of the Internet of Things (IoT) can be easily and quickly eliminated. Instead, IoT can easily take advantage of the decentralized capabilities offered by blockchain networks. From this point onward, future developments of the Internet of Things do not have to rely on centralized services for trust [42-44]. The Internet of Things (IoT) and Blockchain integration frameworks have both been the subject of in-depth research in recent scholarly works. This Blockchain-based Internet of Things can be conceived of from the perspective of cryptography and its requirements of it [40]. These integration changes are depicted in the successive schematics of Figure 3, as shown here.

*The Endpoints for Blockchain are IOT Gateway Devices*

Eventually, in all schemes, all communications will utilize blockchain technology from end-to-end IoT gateways. In addition, this integration strategy enables the authentication of communication between devices linked to various blockchain-enabled gateways. [47]. This tactic is depicted in Figure 3(a). The degree to which decentralisation is achieved via this strategy is not as active or effective as when devices issue transactions onto the blockchain [40].

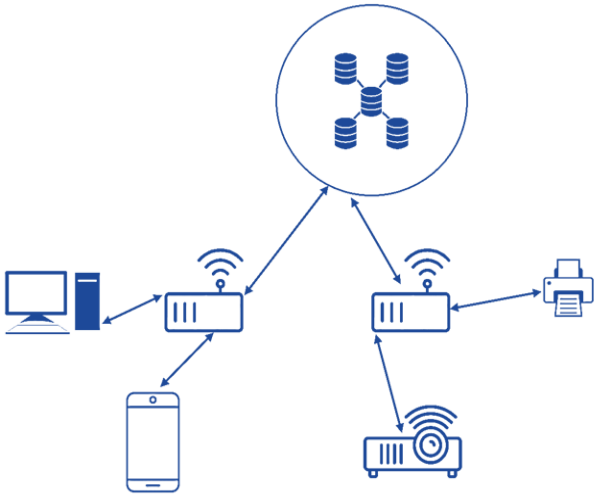

**Fig. 3 a) Gateways devices as end points to Blockchain**

Direct Device transaction-issuers: As shown in Figure 3(b), these devices simply transmit transactions to the blockchain. Each IoT interaction process is recorded on the blockchain to provide secure accountability, resembling the previous method. In this method, IoT devices frequently receive cryptographic capabilities [40]. The key objective or issue at hand is to strike a balance between the increased autonomy of IoT devices and applications and the increased computational complexity of IoT hardware [42].

Hybrid of Cloud-blockchain: These composite designs Utilize blockchain for IoT protocol communications [40]. Cloud consumers and Cloud Service Providers must evaluate the trustworthiness of their collaborating partners before initiating communications [32]. [40] Figure 3(c) primely illustrates this hybrid integration strategy. Fog computing can be supported by hybrid methods to overcome the limitations of blockchain-enhanced IoT networks [45,46].

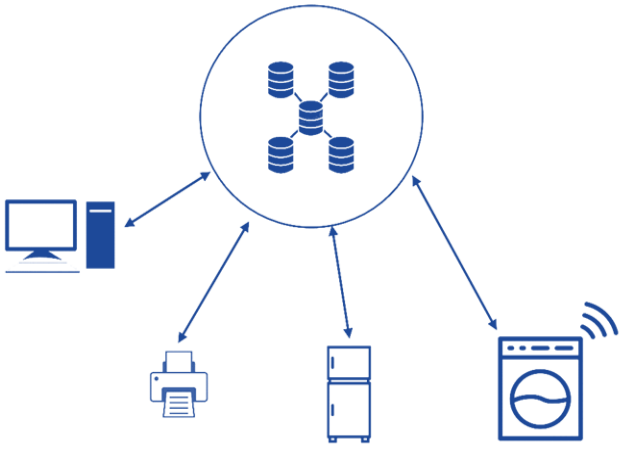

**Fig. 3 b) IoT devices as transaction**

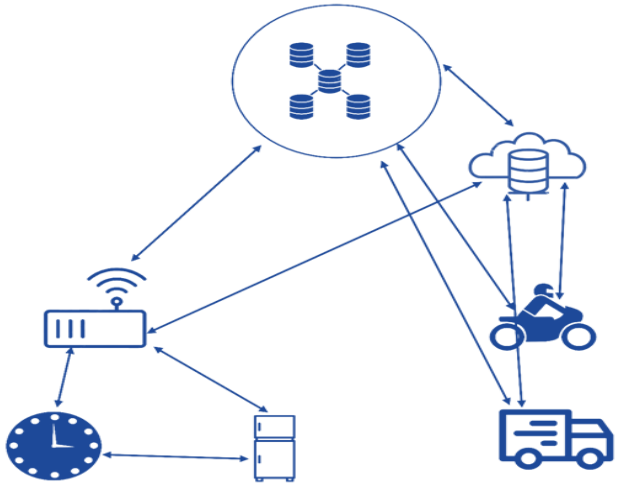

**Fig. 3 c) A hybrid cloud/blockchain**

Trustless IoT Architectures With Blockchains: Since blockchain technology is inherently trustworthy [46-50,63], the two concepts can be used interchangeably. According to section 3.1(key properties of blockchain), Blockchain keeps an immutable or unalterable transactional record that is shared by peers in the same way, suggesting that it may be an appropriate solution for the centralized control of cloud computing [37]. In order to locate a reliable cloud entity under challenging conditions, trust management is a crucial criterion [41]. There is no need to rely on a trusted third party or central consultant to rely on the results of blockchain computation on a collection of data variances.

*2.4.2. Currency-Based*

Blockchain technology's monumental impact on the rise of digital currencies is common knowledge among financial and technological experts. Even though Blockchain technology has applications beyond the realm of currency, ignoring its groundbreaking impact in this area would be irrational. There are billions of dollars invested in the following two currencies, which have started a revolution in today's financial world:

- Bitcoin
- Ethereum

It is a well-established fact that both of these technologies can be classified as examples of public blockchain technology. Bitcoin is a digital currency that competes with gold and other conventional fiat currencies. The following are a few of the most important aspects of bitcoin:

- It's smallest unit is 1 Satoshi=0.00000001BTC
- SHA-256 hashing algorithm is used.
- Proof of work consensus is used.
- Stack-based programming is used to implement smart contracts.
- It has the ability to store monetary value and be a means of payment for goods and services.
- A new token issued, or a transaction lasts for ten minutes.

Ethereum was created as a token to operate smart contracts for lawyer contracts and property ownership. Some of the key points of Ethereum are listed below:

- It's smallest unit is 1wei= 0.000000001Eth.
- Ethash is used.
- Proof of Stake(PoS) consensus is used.
- Turing Complete programming is used to construct smart contracts.
- Applied to generate decentralised applications, such as Decentralised Autonomous Corporations (DAC) and Decentralised Organisations (DO).
- It usually takes between 10 and 20 seconds to complete a transaction or issue a new token.

## 3. Comparitive Study

In the last several years, numerous studies have been undertaken to enhance blockchain technology's consensus processes, application domains, and security over a wide range of depths and metrics. In this section, we compare the results of this study to those of earlier studies, which are summarized in Table 4.

In [20], they studied the fundamental ideas and features of consensus algorithms and the effectiveness and use cases of various consensus techniques in their work. Along with the basic concepts, this research includes consensus conditions and a detailed classification of consensus through its taxonomy. In [21], authors have proposed a solution taxonomy of decentralised consensus algorithms for diverse CPS applications in their work. They have covered practically all of the fundamental components of consensus; however, in this research, it has been highlighted that blockchain as a solution to the CAP theorem in distributed technologies.

The research [22] discusses how approaches to consensus and blockchain architecture are evolving. They have demonstrated the framework and taxonomy of consensus mechanisms; furthermore, we have analyzed how the most prominent consensus mechanisms, together with the proof-based and vote-based classification, vary with various blockchain-related metrics. The authors of the study [23] provide a thorough analysis of the most recent consensus protocols with an emphasis on both the development of mechanisms for reward and the design of distributed consensus mechanisms. However, this article has demonstrated the technical details using taxonomies, such as proof-based, vote-based, and further classifications, so one can easily realize the importance of consensus mechanisms and choose a particular consensus based on their needs. The major goal of the paper [2] is to give an in-depth rundown of many applications of Blockchain technology for academic research. However, this research discussed the applications and grouped them into two primary domains, the currency domain and the non-currency domain, for better understanding [60].

**Table 4. Comparision with existing words**

| Blockchain-based survey contributions | Recent Survey articles | Features Discussed | | | Addressed in this article |
|---|---|---|---|---|---|
| | | Security aspects w.r.t trust and immutability. | Taxonomy of Consensus Mechanisms | Applications in various domains | |
| Mechanisms for Decentralised Consensus in Cyber-Physical Systems | [21] | ✓ | ✓ | × | ✓ |
| Use Cases, Challenges, and Solutions for the Blockchain Architecture and Consensus Protocols | [22] | × | ✓ | ✓ | ✓ |
| Blockchain Consensus Algorithm | [20] | × | ✓ | × | ✓ |
| Blockchain network's management of consensus mechanisms and mining tactics | [23] | ✓ | ✓ | ✓ | ✓ |
| Applications and security privacy Challenges | [2] | ✓ | × | ✓ | ✓ |

## 4. Conclusion

Since the seminal and optimistic paper [1] not only introduces bitcoin but also illustrates the working mechanism of Blockchain technology. As a result, we have compiled a list of references ranging from [1] to recent studies so that we can compose a review article. This research paper aims to give readers a thorough understanding of the fundamentals of blockchain technology, including its major characteristics, different types of blockchains, consensus methods, and applications across various industries. The key features of blockchain and the types of blockchain networks based on application scenarios are presented in sub-section 2 of Fundamentals of Blockchain, respectively. Blockchain technology's peer-to-peer nature makes it more trustworthy in the public territory. Blockchain's consensus technique, on the other hand, is crucial for solving distributed-systems problems and keeping users' trust in the system intact. Subsection 2 presents the consensus mechanisms' taxonomy and details. As it was demonstrated in subsections 2.4.1 and 2.4.2, blockchain technology can be utilized in a wide variety of contexts within the contemporary digital world. These contexts range from the high-end cryptocurrency domain to crucial societal segments. In the third section, a summary and a table with brief explanations have been provided. Researchers who want to start working in these fields will find this work insightful. Despite its many benefits, blockchain is still a young technology that requires more work to scale and adapt. Blockchain provides many benefits, but there are also many technical obstacles. These include issues with block capacity, transaction confirmation time, and transaction throughput. Finding an appropriate balance between enhancing performance and protecting users' privacy will be a challenge for blockchain's future improvements.

## Acknowledgments

The joy and delight that comes with completing a work would be incomplete without mentioning the people who made it possible, whose persistent direction and support crowned our effort with accomplishment. We would like to convey our heartfelt gratitude to the All India Council for Technical Education (AICTE) for providing a Doctoral Fellowship to support our research.

We are indeed grateful to Dr. Vidyashankar. S, Vice Chancellor of VTU Belagavi, for his help, motivation, and encouragement in completing this paper.

We are grateful to Dr. S L Deshpande, Chairperson of VTU-Belagavi, for guiding and providing the essential direction and support to complete this task.

## References

[1] Satoshi Nakamoto, "*Bitcoin:A Peer-to-Peer Electronic Cash System*," Decentralized Business Review, 2008. [Google Scholar] [Publisher Link]

[2] Bhabendu Kumar Mohanta et al., "Blockchain Technology: A Survey on Applications and Security Privacy Challenges" *Internet of Things*, vol. 8, p. 100107, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Yijun zou et al., "Focus on Blockchain: A Comprehensive Survey on Academic and Application," *IEEE Access*, vol. 8, pp. 187182–187201, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Imran Bashir, *Blockchain 101 Mastering Blockchain-Distributed ledger Technology*, Decentralization and Smart Contracts Explained, 2nd Edition, Expert Insight, pp. 11-40 2018.
[5] CISCO, Blockchain Explained. [Online]. Available: https://www.cisco.com/c/en_uk/solutions/executive-perspectives/strategic-technology-trends/blockchain-explained.html
[6] Blockchain Definition and Analogy World Web Consortium. [Online]. Available: https://subscription.packtpub.com/book/data/layered-structure-of-theblockchain-architecture-Introduction
[7] IBM Blockchain. [Online]. Available: https://www.ibm.com/in-en/blockchain
[8] Toqeer Ali Syed et al., "A Comparative Analysis of Blockchain Architecture and Its Applications: Problems and Recommendations," *IEEE Access*, vol. 7, pp. 176838-176869, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[9] Yinsheng Li, "Emerging Blockchain-based Applications and Techniques," *Service Oriented Computing Applications*, vol. 13, pp. 279–285. 2019. [CrossRef] [Google Scholar] [Publisher Link]
[10] Stephan leible et al., "A Review on Blockchain Technology and Blockchain Projects Fostering Open Science," *Frontiers in Blockchain*, vol. 2, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[11] Henry Rossi Andrian, Novianto Budi Kurniawan, and Suhardi, "Blockchain Technology and Implementation: A Systematic Literature Review," *International Conference on Information Technology Systems and Innovation (ICITSI)*, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[12] Jorg Weking et al., "The Impact of Blockchain Technology on Business Models– A Taxonomy and Archetypal Patterns," *Electronic Markets*, vol. 30, pp. 285–305, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[13] Shafaq Naheed Khan et al., "Blockchain Smart Contracts: Applications Challenges, and Future Trends," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2901–2925, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[14] C.M. Rakshitha, "Scope and Limitations of Ethical Hacking and Information Security," *International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[15] Pierluigi Martino, "Blockchain Technology: Key Features and Main Applications," *Blockchain and Banking*, pp. 9-31, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[16] Noe Elisa et al., "A Framework of Blockchain-based Secure and Privacy-preserving E-Government System," *Wireless Networks*, vol. 29, pp. 1005-1015, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[17] U. Gokulahari et al., "Decentralized Application," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 7, pp. 45-50, 2020. [CrossRef] [Publisher Link]
[18] Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis, "A Systematic Literature Review of Blockchain-based Applications: Current Status, Classification and Open Issues," *Telematics and Informatics*, vol. 36 pp. 55-81, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[19] Xiang Fu, Huaimin Wang, and Peichang Shi, "A Survey of Blockchain Consensus Algorithms: Mechanism, Design and Applications," *Science China Information Sciences*, vol. 64, p. 121101, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[20] Du Mingxiao et al., "A Review on Consensus Algorithm of Blockchain," *IEEE International Conference on Systems, Man and Cybernetics*, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[21] Umesh Bodhke et al., "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems," *IEEE Access*, vol. 8, pp. 54371-54401, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[22] Leila Ismail, and Huned Materwala, "A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions," *Symmetry*, vol. 11, no. 10, p. 1198, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[23] Wenbo Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol.7, pp. 22328-22370, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[24] Shubhani Aggarwal, and Neeraj Kumar, "Cryptographic Consensus Mechanisms," *Advances in Computers*, vol. 121, pp. 211-226, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[25] Friedhelm Victor, Peter Ruppel, and Axel Kupper, "A Taxonomy for Distributed Ledger Analytics," *IEEE Computer Society Digital Library*, vol. 54, pp. 30-38, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[26] Jeff Nijsse, and Alan Litchfield, "A Taxonomy of Blockchain Consensus Methods," *Cryptography*, vol. 4, no. 4, p. 32, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[27] Sohail Jabbar et al., "Blockchain-enabled Supply Chain: Analysis, Challenges,and Future Directions," *Multimedia Systems*, vol. 27, pp. 787–806, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[28] Yanqi Zhao et al., "Secure Pub-Sub: Blockchain-based Fair Payment with Reputation Reliable Cyber Physical Systems," *IEEE Access*, vol. 6, pp. 12295-12303, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[29] Rui Guo et al., "Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems," *IEEE Access*, vol. 6, pp. 11676-11686, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[30] Haikel Magrahi et al., "NFB: A Protocol for Notarizing Files over the Blockchain," *9th IFIP International Conference on New Technologies, Mobility and Security*, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[31] Rim Ben Fekih, and Mariam Lahami, "Application of Blockchain Technology in Healthcare: A Comprehensive Study," *International Conference on Smart Homes and Health Telematics*, pp. 268-276, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[32] Praveen S. Challagidad, and Mahantesh N. Birje, "Multi-dimensional Dynamic Trust Evaluation Scheme Forcloud Environment," *Computers & Security*, vol. 91, p. 101722, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[33] J. Jhanavi, and M. Dakshayini, "Blockchain Implementation for Storage," *SSRG International Journal of Mobile Computing and Application*, vol. 5, no. 2, pp. 9-12, 2018. [CrossRef] [Publisher Link]
[34] Yan Zhuang et al., "Generalizable Layered Blockchain Architecture for Health Care Applications: Development, Case Studies, and Evaluation," *Journal of Medical Internet Research*, vol. 22, no.7, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[35] Muhammad Aamir et al., "Blockchain Based Academic Records Verification in Smart Cities," *Wireless Personal Communications*, vol. 113, pp. 1397-1406, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[36] Zina Balani, and Hacer Varol, "Cloud Computing Security Challenges and Threats," *IEEE International Symposium on Digital Forensics and Security (ISDFS)*, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[37] A. Gayathiri, J. Jayachitra, and S. Matilda, "Certificate Validation using Blockchain," *7th International Conference on Smart Structures and Systems (ICSSS)*, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[38] Meng han et al., "A Novel Blockchain-based Education RecordsVerification Solution," *The 19th Annual SIG Conference on Information Technology Education*, pp. 178-183, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[39] Ahmed AfifMonrat, Olov Schelen, and Karl Andersson, "A Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities," *IEEE Access*, vol. 7, pp. 117134-117154, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[40] Muhammad Salek Ali et al., "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676-1717, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[41] Mahantesh N. Birje, and Vijay L. Hallappanavar, "Trust Management Techniques, Models and Attacks in Cloud," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 4, pp. 2647-2655, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[42] Vishal sharma, and Niranjan Lal, "A Detail Dominant Approach for IoT and Blockchain with their Research Challenges," *IEEE International Conference on Emerging Trends in Communication, Control and Computing (ICONC3)*, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[43] Anil Lamba et al., "Mitigating IoT Security and Privacy Challenges using Distributed Ledger based Blockchain Technology," *International Journal for Technological Research in Engineering*, vol. 4, no. 8, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[44] Nallapaneni Manoj Kumara, and Pradeep Kumar Mallick, "Blockchain Technology for Security Issues and Challenges in IoT," *Procedia Computer Science*, vol. 132, pp. 1815-1823, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[45] Guy Zyskind, Oz Nathan, and Alex Pentland, "Enigma: Decentralized Computation Platform with Guaranteed Privacy," *Cryptography and Security*, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[46] Bin Liu et al., "Blockchain Based Data Integrity Service framework for IoT Data," *IEEE International Conference on Web Services (ICWS)*, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[47] Pascal Urien, "Towards Secure Elements for Trusted Transactions in Blockchain and Blochchain IoT (BIoT) Platforms," *Fourth International Conference on Mobile and Secure Services (Mobisecserv)*, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[48] Aymen Boudguiga et al., "Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain," *IEEE European Symposium on Security and Privacy on Blockchain Workshops (Euro S&PW)*, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[49] Bin Yu et al., "IoT Chain: Establishing Trust in the Internet of Things Ecosystem using Blockchain," *IEEE Cloud Computing*, vol. 5, no. 4, pp.12-23, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[50] Pim Otte, Martijin de Vos, and Johan Pouwelse, "Trustchain: A Sybil-resistant Scalable Blockchain," *Future Generation Computer Systems*, vol. 107, pp. 770-780, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[51] Houda Lhore et al., "Blockchain Technology as a Possible Solution to IoT Security Issues," *International Journal of Engineering Trends and Technology*, vol. 71, no. 1, pp. 152-163, 2023. [CrossRef] [Publisher Link]
[52] Peng Cheng Wei et al., "Blockchain Data-based Cloud Data Integrity Protection Mechanism," *Future Generation Computer Systems*, vol. 102, pp. 902-911, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[53] Emmanuel Boateng Sifah et al., "A Blockchain Approach to Ensuring Provenance to Outsourced Cloud Data in a Sharing Ecosystem," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1673-1684, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[54] Haiyang Yu et al., "Efficient Continuous Big Data Integrity Checking for Decentralized Storage," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1659-1673, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[55] Walid Miloud Dahmane, Samir Ouchani, and Hafida Bouarfa, "Guaranteeing Information Integrity and Access Control in Smart Cities through Blockchain," *Journal of Ambient Intelligence and Humanized Computing*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[56] Neha Jain, and R.R. Sedamkar, "A Blockchain Technology Approach for the Security and Trust Trade Finance," *14th IEEE International Conference on Innovations in Information Technology (IIT)*, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[57] Mazin Debe et al., "Blockchain-Based Decentralized Reverse Bidding in Fog Computing," *IEEE Access*, vol. 8, pp. 81686-81697, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[58] Maha M. Althobaiti, "Blockchain Adoption Opportunities in Healthcare Sector," *International Journal of Engineering Trends and Technology*, vol. 68, no. 10, pp. 117-120, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[59] Saikat Mazumder, and Amiya Bhaumik, "Blockchain: Transforming Supply Chain Management Amidst Covid-19," *International Journal of Engineering Trends and Technology*, vol. 70, no. 6, pp. 100-105, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[60] M. N. Birje et al., "A Review on Layered Architecture and Application domains of Blockchain Technology," *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[61] Guang Chen et al., "Exploring Blockchain Technology and Its Potential Applications for Education," *Smart Learning Environments*, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[62] Mahantesh N. Birje et al., "Cloud computing Review: Concepts, Technology, Challenges and Security," *International Journal of Cloud Computing*, vol. 6, no. pp. 32-57, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[63] Feng Tian, "A Supply Chain Traceability System for Food Safety based on HACCP, Blockchain & Internet of Things," *International Conference on Service Systems and Service Management*, 2017. [CrossRef] [Google Scholar] [Publisher Link]