Journal of Manufacturing Systems 77 (2024) 612–638

Contents lists available at ScienceDirect

Journal of Manufacturing Systems

journal homepage: www.elsevier.com/locate/jmansys

Review

# Leveraging the usage of blockchain toward trust-dominated manufacturing systems

Philip Samaha [a], Fadi El Kalach [a], Ramy Harik [b,*]

[a] University of South Carolina, Department of Mechanical Engineering, Columbia, South Carolina
[b] Clemson University, Clemson Composites Center, Greenville, South Carolina

ARTICLE INFO

*Keywords:*
Blockchain technology
Smart Manufacturing
Cybersecurity
Cyber-Physical Infrastructure
Supply Chain Management

ABSTRACT

Smart manufacturing has transformed the role of data in manufacturing, with a significant focus on secure data infrastructure. As factories engage with external data sources, cybersecurity becomes crucial. Blockchain technology is introduced to safeguard this infrastructure, ensuring secure and transparent data flow, which is vital for industries like pharmaceutical, aerospace, automotive, and electronics manufacturing. This review provides a comprehensive taxonomy of blockchain architectures, analyzing their working modes, strengths, and weaknesses while identifying appropriate use cases. It also examines consensus algorithms, categorizing them as either crash fault tolerant (CFT) or Byzantine fault tolerant (BFT) and further classifies them based on whether they are proof-based or voting-based. The review explores the intrinsic limitations of blockchain systems and highlights specific manufacturing challenges where blockchain can be instrumental. It also discusses the synergy between blockchain and cybersecurity, emphasizing how they work together to enhance security and accountability. The paper concludes by identifying private blockchain as the most suitable architecture for certain manufacturing applications, particularly in supply chain management and machinery control. A SWOT analysis is conducted on this architecture to provide a detailed understanding of its potential and challenges. The review suggests that while no single consensus algorithm is best universally, each has its own merits depending on the application. Lastly, the SWOT analysis serves as a catalyst for future research, guiding efforts to maximize blockchain's strengths and mitigate its weaknesses in industrial contexts.

## 1. Introduction

A blockchain is an immutable ledger that is shared and decentralized, allowing users to send/receive transactions, data, or information on a peer-to-peer network without relying on a trusted third party, as defined by [1].

The use of blockchain technology was primarily limited to cryptocurrency and electronic banking where the transactions exchanged were financial ones, whereas the data and information trafficked over blockchain system were related to banking information. However, the advent of smart contracts - a blockchain-based application - has expanded the potential use cases of blockchain beyond transactional exchange [2].

To illustrate, businesses and organizations utilize blockchain technology at a private level for securely storing and sharing data, rendering it accessible to any node within a network while maintaining immutability and preventing alteration, even by the data owner. As such, various types of blockchains have arisen to suit different purposes, including permissionless, permissioned, hybrid, and consortium blockchains. As tracking mechanisms are being developed to enhance transparency and ensure authentic data in supply chains, research into the potential applications of blockchain technology within this domain has gained significant traction as evidenced by the increased publications in this domain.

Blockchain technology has the potential to significantly impact the manufacturing industry by enhancing transparency and ensuring data authenticity. Traditional supply chain management models are vulnerable to fraud and counterfeiting, but the transparency offered by blockchain can address these issues through improved traceability and real-time tracking. Additionally, blockchain can eliminate the need for third-party organizations, such as banks or financial institutions, that currently serve as transaction validators. This reduction not only lowers transaction fees but also minimizes the risk of human error in authentication processes. Moreover, manufacturing processes are prone to

* Corresponding author.
*E-mail addresses:* psamaha@email.sc.edu (P. Samaha), elkalach@email.sc.edu (F. El Kalach), harik@clemson.edu (R. Harik).

https://doi.org/10.1016/j.jmsy.2024.10.010
Received 19 September 2023; Received in revised form 21 August 2024; Accepted 13 October 2024
Available online 23 October 2024

various anomalies, and a secure repository for storing defective data is essential for tracing and resolving these issues efficiently. Scholars are increasingly drawn to this field, with a view to leveraging blockchain's capabilities to address the current gaps that exist within supply chains [3].

The integration of machine learning algorithms in complex blockchain networks is crucial for their future development [4]. By utilizing AI, network parameters can be established, and node behavior analyzed, facilitating the identification of potential malicious attacks on the network. Blockchain technology has gained significant attention as a promising solution for augmenting the manufacturing and supply chain landscape [5].

The manufacturing industry faces significant challenges across various sectors, with the ultimate goal being the creation of a sustainable environment that optimizes resource use while delivering the highest possible production quality. To address these issues, it is essential first to identify the specific problems within different sectors of the industry. This paper focuses on exploring solutions to these gaps through the emerging technology of blockchain.

The first contribution of this paper is the development of a centralized taxonomy of current blockchain architectures, including their respective consensus algorithms. This taxonomy will provide a comprehensive understanding of the distinctions between each architecture, highlighting their advantages and disadvantages, and helping to identify the specific gaps each architecture is designed to address. Consensus algorithms, which are at the core of blockchain technology, play a vital role in maintaining the security and synchronization of the database. Therefore, gaining a deep understanding of how these key consensus algorithms function, along with their limitations, is essential for building a robust knowledge base of this technology. These algorithms are classified based on Proof-Based and Voting-Based protocols, as well as on the premises of Crash Fault Tolerance (CFT) and Byzantine Fault Tolerance (BFT). This classification aids in selecting the most appropriate consensus algorithm for specific use cases. This, in turn, aids in identifying the opportunities for effectively implementing blockchain technology in various applications.

The second contribution involves identifying the challenges within various manufacturing sectors, analyzing how these issues impact operations, and discussing how blockchain technology has the potential to address them. Additionally, the paper clarifies the relationship between blockchain and cybersecurity, exploring how these two domains can work together to form a comprehensive security framework.

After outlining the problems, the paper compares different blockchain architectures, quantifying their features to identify the most suitable architecture for the discussed use cases. Following this, a SWOT analysis is conducted on the selected architecture to not only facilitate problem-solution research but also to investigate the solution's properties. Understanding the advantages and disadvantages of the proposed solution is crucial, as it paves the way for further research aimed at addressing any shortcomings and refining the approach.

## 2. Research objectives

The following points summarize the research objectives of this review.

a) Analyze the current blockchain architectures in use and explore their specific details.
b) Review the prominent consensus algorithms and examine the scenarios in which they are applied and the problems they address.
c) Explore the challenges that blockchain systems faces
d) Investigate potential use cases of blockchain in the manufacturing industry
e) Discuss the synergy between blockchain and cybersecurity.
f) From the information gathered through the literature review, determine the most suitable blockchain architecture for the manufacturing industry.
g) Conduct a SWOT analysis for the selected architecture to gain a deep understanding of this type and its implementation.

Once the initial objectives were identified, the search for relevant publications began by using specific keywords to gather pertinent information. The key terms used for each section are highlighted in Fig. 1. After identifying and selecting papers relevant to the topics, they were classified by section, and the paper was subsequently written based on these findings.

The literature review was initiated by conducting an extensive search for relevant topics, followed by identifying and categorizing papers according to the sections where they would be applied. As illustrated in Fig. 1, the number of references used in each section is represented along with the most used key words for each section. Fig. 2 shows the publication years of the references, with the majority of the sources dating from 2018 to 2023.

## 3. Taxonomy

### 3.1. Permissionless or public blockchain

#### 3.1.1. Definition

Public blockchain is known as a transparent and secure decentralized database network [6]. Its alternative naming "permissionless blockchain" stems from its open-source nature that allows individuals to join, access, and interact with the network without relying on specific credentials or permissions [7]. This model is particularly advantageous for public use, as users can easily create their own addresses and data, then engage with the network in an unsupervised and uncensored manner [8]. The lack of identity verification enables members to maintain their anonymity. In contrast, earlier system models relied on a centralized trusted third party to validate all transactions [9]. The decentralized nature of permissionless blockchains allows members or nodes to directly send and receive transactions without a trusted intermediary. This architecture is commonly used in financial platforms such as Bitcoin and Ethereum [10]. One of the most well-known consensus algorithms in public blockchains is Proof-of-Work (PoW), which involves data mining and is known for its significant computational demands that limit scalability [11]. An alternative solution that reduces power consumption and improves scalability is the implementation of a different consensus mechanism, such as Proof-of-Stake which requires much less power while providing comparable security to PoW [12].

#### 3.1.2. Advantages

One of the key benefits of permissionless blockchains is their independence from centralized organizations [13]. This means that even if the entity that established and initiated the blockchain withdraws its contributions and exits the network, the blockchain system will continue to operate. This eliminates any evidence of centralization, enhancing the system's trustworthiness and protecting it from domination by any single party or group. Consequently, decisions within the network are not made by a single authoritative group but are agreed upon through a consensus algorithm where all nodes participate in decision-making [14]. These algorithms will be discussed in the third section of this literature review.

Furthermore, the replication of transactions across all nodes in the network makes blockchain immutable and resilient [15].

Given the inherent transparency of public blockchains, where all transactions are visible to every node within the network, privacy concerns require anonymity measures for participants. To protect the identities of individuals involved in transactions, users can generate new key pairs (public and private keys) for each transaction which prevents direct connections between transactions and individual participants

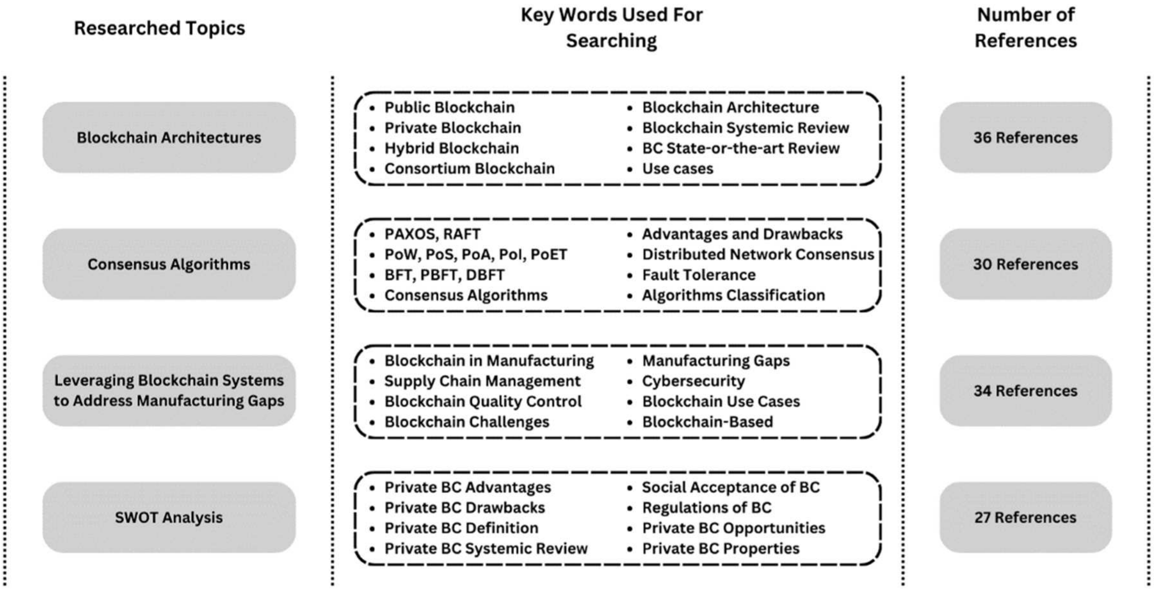


**Fig. 1.** Literature review strategy.

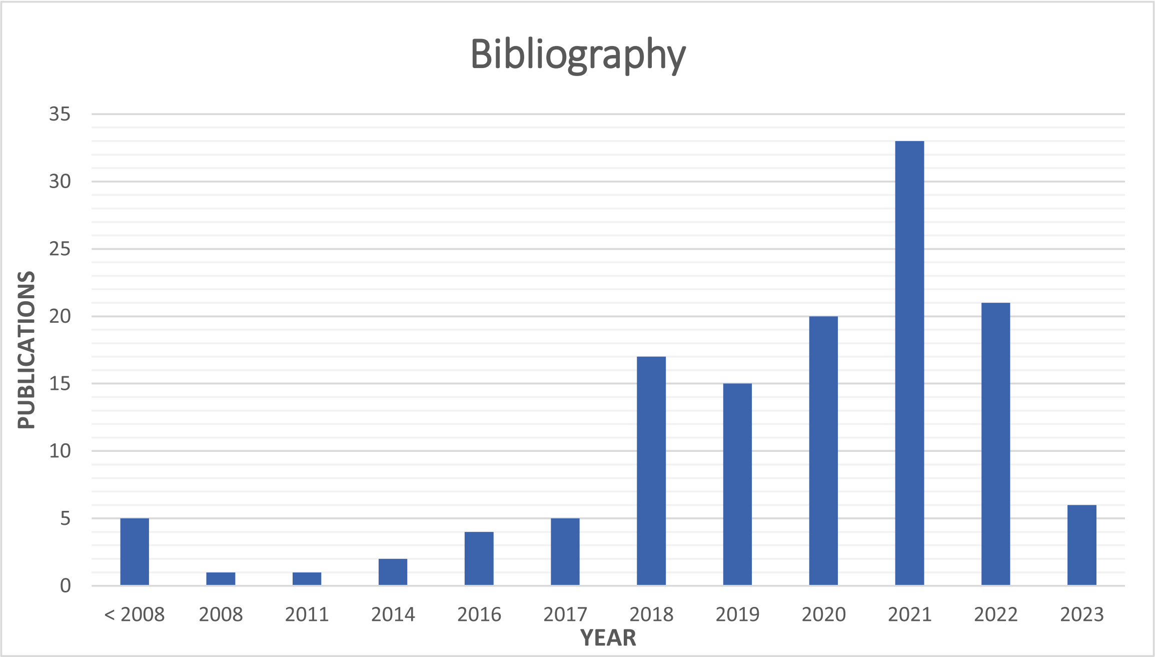


**Fig. 2.** Number of publications vs. year of publications.

[16]. The public key functions as a pseudonym for nodes on the blockchain.

An additional benefit of this architectural design pertains to the quantity of nodes present in the network. As previously stated, the foundational principle of blockchain revolves around decentralization, with security being a direct byproduct of data replication rather than centralized storage—where vulnerabilities, such as breaches or unauthorized alterations, may manifest. Consequently, a high number of data replications indicates a high-security index. However, it is imperative to acknowledge that an excessive number of nodes within a network can negatively affect the performance of the system. Thus, it becomes apparent that the scalability of the network is not boundless [13].

All the stated properties of public blockchain imply a high-security standard that is reliable enough to be applied in financial systems like Bitcoin for example.

### *3.1.3. Disadvantages*

One of the primary drawbacks of permissionless blockchains is their high energy consumption, which stems from the substantial power required to add blocks to the ledger [15].

Given that access control is beyond the purview of organizations, the risk of hackers gaining control over 51 % or more of the network and the ability to manipulate data is heightened, however, this type of blockchain is mostly used on a public scale where the number of nodes is usually very high which makes it difficult for a bad actor to gain control over 51 % of the network while considering the other security layers in blockchain discussed in the definition, thus, this possibility cannot be omitted but it is unlikely to happen [17].

Additionally, the computational burden and time-consuming nature of proof-of-work authentication required to verify blocks significantly slow down the blockchain process, as it involves solving complex mathematical problems to solve the hash of the blocks [18]. Resulting in low throughput for this type of blockchain.

Scalability plays a prominent role in the advancement of this technology. However, as mentioned before, a high number of nodes in the network will significantly increase the security of the system but decrease its performance, thus, scaling a system comes at a cost in its security [19].

Furthermore, operating a node on a permissionless blockchain is technically difficult and requires a lot of resources. Thus, the complexity of managing the storage, bandwidth, and software updates on these nodes poses a significant challenge for non-technical users [20].

#### 3.1.4. Use cases

The initial implementation of blockchain technology was a public permissionless blockchain system, with the most notable use case being its application in the cryptocurrency realm, specifically Bitcoin [1].

Over the past decade, a significant amount of research has been conducted to identify areas where blockchain could be utilized to great effect. As a result of this research, several gaps in various fields have been identified, that blockchain can be well-suited to address, given its ability to offer transparency and trust. This is especially relevant for non-profit or non-governmental organizations, where these aspects are of utmost importance and blockchain can help to fill these gaps [21]. For example, charitable donations.

This blockchain architecture is being investigated to fills gaps in applications such as Insurance [22], Medical Care [23], Cloud Computing [24] and IoT [25].

Additionally, the usage of blockchain could be leveraged to be used in e-voting [26], improving the security and transparency in the electronic voting processes.

Public blockchain could be used as well for the tokenization of assets. This refers to representing ownership of physical or digital assets on a distributed ledger [27].

*Note:* A P2P network also known as a peer-to-peer network is an architecture of a network that is composed of a group of computers where each of them acts as a node that shares data on the network. This architecture differs from others in its decentralized nature where there is no need for a centralized server to communicate and store the data, but rather each node acts as a server storing the files that it shares, the network is said to be fully decentralized when the nodes communicate and store data, along with these nodes having the ability to offer services usually executed on a centralized servers [28].

Fig. 3 above summarizes the advantages, disadvantages and use cases for the Permissionless or Public blockchain architecture discussed in section 2.1.

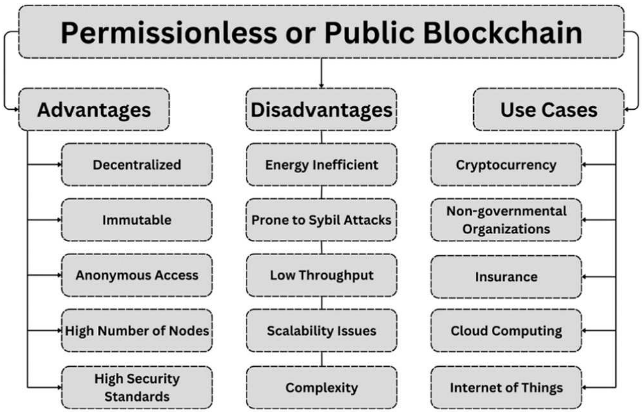


**Fig. 3.** Permissionless or public blockchain summary.

### 3.2. Permissioned or private blockchain

#### 3.2.1. Definition

A permissioned blockchain is a type of blockchain architecture that functions within a non-public or proprietary environment. The network is owned and controlled by organizations or enterprises who have the authority to determine the participants and their roles within the network [29]. This model is specifically designed for industrial use and users are not permitted to join the network unless they are granted permission and assigned a specific role [30]. Permissioned blockchain uses contracts to predetermine the behavior of members on the network, ensuring constructive and positive contributions and enabling highly efficient consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT) [31]. Unlike permissionless blockchain, permissioned blockchain does not require mining, resulting in an energy-efficient system with low power overhead.

#### 3.2.2. Advantages

The architecture of this type of blockchain is centered on permissions, as the name suggests. The organization that adopts this system has the authority to grant permissions to participants on various levels, in addition to establishing security policies determining authorized personnel and how they access the network [21]. These features allude to a private and proprietary blockchain that is owned by the organization. For instance, the organization can allocate a specific user with access or push data capabilities into the system, while preventing unauthorized third parties from accessing sensitive information.

A private blockchain can process transactions and store data rapidly when compared to a public blockchain. Thus, having a high throughput. Which is advantageous when scaling up the system [32].

As mentioned in the definition of private blockchain section, this blockchain architecture does not require mining or extensive computing resources to validate the blocks, making permissioned blockchain energy efficient, unlike public architecture [33].

The primary shared beneficial attribute between public and private blockchains is their high security standards. While public blockchains achieve security through the utilization of the "PoW" consensus algorithm and the high number of nodes in the network, private blockchains attain security through their proprietary nature. In private blockchain architectures, the roles of each node are tightly controlled and predefined. Additionally, these networks typically maintain a restricted number of nodes.

Another shared property between public and private blockchain is the foundation of these blockchain systems. Private blockchain store data on a ledger distributed among all the nodes in the network, thus achieving immutability and transparency.

#### 3.2.3. Disadvantages

When blockchain was initially introduced, its primary characteristic was decentralization. However, the validation and authentication of data and transactions are performed on centralized nodes in private blockchain architectures [8].

Additionally, private blockchain systems typically have a smaller number of nodes than public blockchain networks, resulting in less security. If a certain percentage of the nodes are corrupted, the consensus mechanism could be compromised [34].

Anonymity is not a feature of permissioned blockchains because identities must be verified in this type of networks [35]. Furthermore, the source code of blockchain is confidential and cannot be accessed by users for verification and validation.

The importance of having an anonymous identity in such network lies behind securing one’s identity and crucial information, as discussed in this review, any data that is registered or recorded in the blockchain database is immutable and cannot be deleted whatsoever, thus keeping important personal data in blockchain can be dangerous and breach individual’s privacy in some cases.

#### 3.2.4. *Use cases*

Private blockchain systems are increasingly being adopted by organizations that require secure exchange of data and transactions, while also ensuring privacy by restricting information circulation to only the nodes assigned to the network. This architecture is particularly well-suited for supply chain management, where many organizations are developing blockchain systems to improve efficiency and transparency. The fast speed of data processing and real-time monitoring capabilities make private blockchain a desirable option for supply chain applications [32]. Supply Chain Management (SCM) encompasses the entire flow of goods, services, and information, beginning with raw materials and extending through to the end consumer. It is a fundamental component of the manufacturing industry.

This architecture's framework shows considerable potential in addressing challenges related to factory-to-factory communications. The future of manufacturing is based on collaborative efforts among diverse factories to streamline processes effectively and expedite operations. Factory-to-factory communication involves the exchange of various types of data between collaborating factories, which may include sensor data, transactional data, inventory data, and other relevant information. In this context, inventory data plays a crucial role in demand forecasting. When multiple factories work together to manufacture a specific product, with each organization contributing different components, having streamlined and secure communication channels is essential. This ensures effective collaboration and minimizes the likelihood of errors arising from inaccurate forecasting, miscommunication, or faulty data. However, the susceptibility to security breaches in the communication channels connecting these factories poses a significant risk [36]. Such breaches can lead to substantial losses, particularly when involving malicious or erroneous orders, potentially causing disruptions and financial losses. Blockchain has the potential to contribute to securing these channels and mitigate these risks.

The safeguarding of patient privacy necessitates a high level of security for medical records. Consequently, a private blockchain system can serve as a secure repository for these records, granting access permissions solely to the respective patient, thereby ensuring the confidentiality and integrity of their medical data [37].

Fig. 4 above summarizes the advantages, disadvantages and use cases for the Permissioned or Private blockchain architecture discussed in section 2.2.

### 3.3. *Hybrid blockchain*

#### 3.3.1. *Definition*

Hybrid blockchain refers to a blockchain design that incorporates both public and private blockchain functionalities. The foundation of this system is a private permissioned blockchain, which is complemented by a public permissionless blockchain. This combination enables organizations to determine who has access to specific confidential data stored on blockchain, while also retaining the ability to regulate which information is made available to the public [38]. It is important to note that the hybrid blockchain is owned by an entity, and even its owner is unable to modify or manipulate transactions or data.

#### 3.3.2. *Advantages*

The utilization of a permissioned blockchain as the core of the hybrid blockchain structure ensures that the system operates within a private environment, thereby preventing external hackers from initiating a Sybil attack [39].

All data is contained within the network and can be verified through smart contracts, thus ensuring privacy protection while facilitating the exchange of information between parties [39].

In addition, the absence of mining in this type of blockchain enables cost-effective and expeditious secure transactions and data exchange. Compared to other blockchain designs, hybrid architecture is relatively more scalable [39].

#### 3.3.3. *Disadvantages*

Despite the secure nature of the information stored on the network, its validation process lacks automation and is reliant on smart contracts. This approach increases the risk of information being concealed or obscured by limiting access to the data [40].

Since this architecture is a proprietary system since it is based on private blockchain architecture, thus it lacks anonymity since all users should be verified before existing on the network. In addition, this type has the shortcoming of having low number of nodes since it is founded on private architecture allowing only specific user to join the network.

#### 3.3.4. *Use cases*

The hybrid blockchain has several noteworthy use cases, such as the energy, agriculture, construction, manufacturing, supply chain, industries which enables private system operation while allowing selective public access to information. Similarly, in military and governmental applications it offers compelling advantages. Additionally, a hybrid blockchain is a suitable solution for storing medical records [38]. Furthermore, hybrid blockchain can be used as a foundation for digital identity management solutions.

Fig. 5 above summarizes the advantages, disadvantages and use cases for the Hybrid blockchain architecture discussed in section 2.3.

### 3.4. *Consortium blockchain*

#### 3.4.1. *Definition*

Consortium blockchain is like hybrid blockchain in that it combines aspects of both private and public blockchains. However, it differs in terms of restricted access. This network is only accessible to a specific

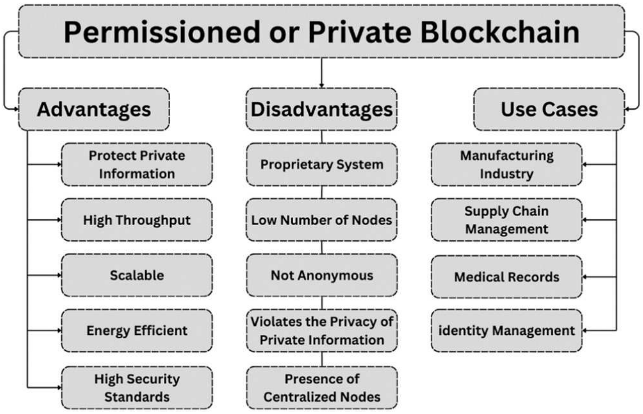


**Fig. 4.** Permissioned or private blockchain summary.

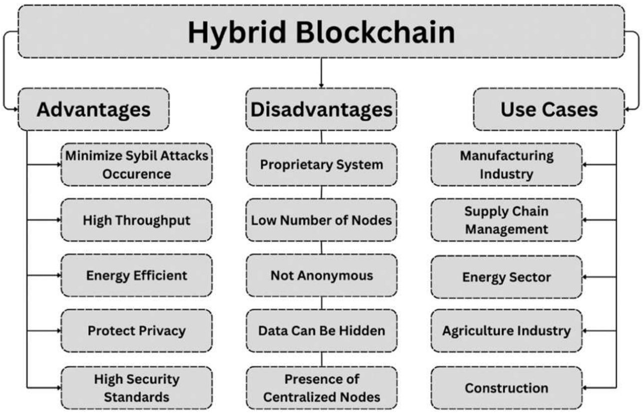


**Fig. 5.** Hybrid blockchain summary.

group of users, but it is not centralized and owned by a single company, unlike the hybrid blockchain. This eliminates the possibility of the network being controlled by a single entity. Consensus on this network is established through pre-determined validator nodes, which are responsible for initiating, receiving, and validating transactions. Other members are authorized to only initiate or receive transactions [41]. The consortium blockchain has the potential to be utilized in any organization that provides services to end-users and requires private data storage, selective user access, and data privacy. This type of blockchain can fulfill these requirements effectively.

#### *3.4.2. Advantages*

Consortium blockchains, like private and hybrid blockchains, are built on private information that can be verified by allowing access to designated members and users. However, it differs from other blockchain types by virtue of its decentralized structure, which precludes any possibility of monopolization. It has a high throughput since the consensus mechanisms used in this architecture do not require extensive resources. Immutability is one of the core properties among all the architectures of blockchain including consortium blockchain. As mentioned in the definition, consortium blockchain is not a proprietary system which plays to its advantage of being more reliant on and more secure.

#### *3.4.3. Disadvantages*

Despite its robust security and the possibility of limited public access with special permissions, this blockchain architecture is less transparent than public blockchains. Moreover, if a member node is corrupted or hijacked, this significantly increases the risk of the network being compromised. As private and hybrid architectures are not anonymous, consortium blockchain shares this property as well. In addition, data can be hidden in this network if permission to access this data is not given, thus, making it less transparent than other types.

#### *3.4.4. Use cases*

This blockchain architecture is well-suited for the finance and insurance sectors, where it can facilitate asset trading and the issuance of insurance policies. Additionally, it has applications in the energy sector, such as ensuring the authenticity of data in solar systems. In the mobility sector, blockchain can be used to store asset information, and in logistics, it can track assets throughout the distribution network. Moreover, this type of blockchain is beneficial for collaborative projects involving multiple entities [41].

Fig. 6 above summarizes the advantages, disadvantages and use cases for the Consortium blockchain architecture discussed in section 2.4.

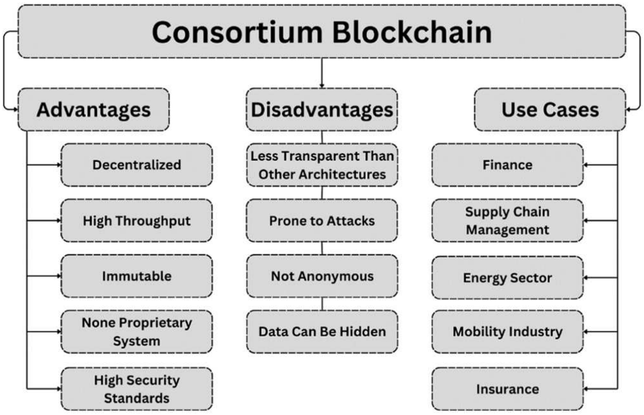


**Fig. 6.** Consortium blockchain summary.

### *3.5. Taxonomy summary*

The Venn diagram below visualizes the common properties between the different blockchain architectures. As presented in Fig. 7, the fundamental specifications are shared among all the different architectures: high-security standards, immutability, block structure, transparency, etc. However, we can observe as well that the least commonality resides mostly when comparing public with private and consortium architecture.

## 4. Consensus algorithms

The two primary types of blockchains are public and private blockchains. Initially, the consensus mechanisms of these systems were designed as a challenging computational puzzle to be solved by the node responsible for verifying the authenticity of a block being added to blockchain. This algorithm is called Proof of Work (PoW) and requires significant computational power, time, and effort to solve. Currently, many cryptocurrencies rely on this consensus algorithm, which provides high levels of security but is not particularly energy or time efficient. Numerous consensus algorithms were developed aiming to find a balance that provides high security and increases its efficiency in terms of energy and time requirements. This section lists a wide range of consensus algorithms used in public and private blockchain architectures, delving into their security requirements which is the maximum tolerable faulty nodes for each algorithm, then expanding on their respective properties.

### *4.1. Proof-based consensus algorithms*

In synchronous blockchain networks, all nodes are assumed to be operating under a shared time clock with minimal or no delay. These networks ensure that state updates are completed at the end of each cycle. On the other hand, asynchronous networks do not guarantee the completion of each round of the algorithm and will continue to run until the block is created and published [42]. Proof-based consensus algorithms are probabilistic mechanisms that typically operates on asynchronous communication networks such as the internet, additionally, these algorithms are suitable for public applications [43]. Proof-based consensus algorithms include but are not limited to; Proof of Work (PoW), Proof of Stake (PoS), Proof of Activity (PoA), Proof of Importance (PoI), and Proof of Elapsed Time (PoET). The mentioned algorithms above will be detailed in the subsequent section.

#### *4.1.1. Proof of work (PoW)*

PoW is the earliest consensus mechanism used in bitcoin [44]. The proof of work is a consensus mechanism that requires a node in the network to solve a convoluted computational problem [45]. All the nodes on the network are allowed to participate in the process, and the first node to solve that problem is allowed to mine the block, and the work done by the node is rewarded. The nodes in a network can be regular computers, servers, Internet of Things (IoT) devices, or any other device that can connect to the network and generate or analyze data. The work usually done by these nodes is mining which is solving for the hash of the block, and the reward is a percentage of the transaction [46]. Within cryptocurrency, the difficulty of these problems is constantly regulated to keep the rate of inflation of the coins under control. This task is challenging because it involves different considerations, mainly the difficulty of the problem should be such as hard enough to endure spam or Sybil attacks (which is the usage of the same node to operate numerous fake identities), but at the same time flexible enough not to disrupt the generation of new blocks at the required rate [47]. Overall, PoW provides reliable security for the system, but its disadvantage is that it requires considerable time and a large amount of energy [48]. This algorithm's fault tolerance is 51 %, which indicates that this algorithm will ensures security and authenticity under the assumption

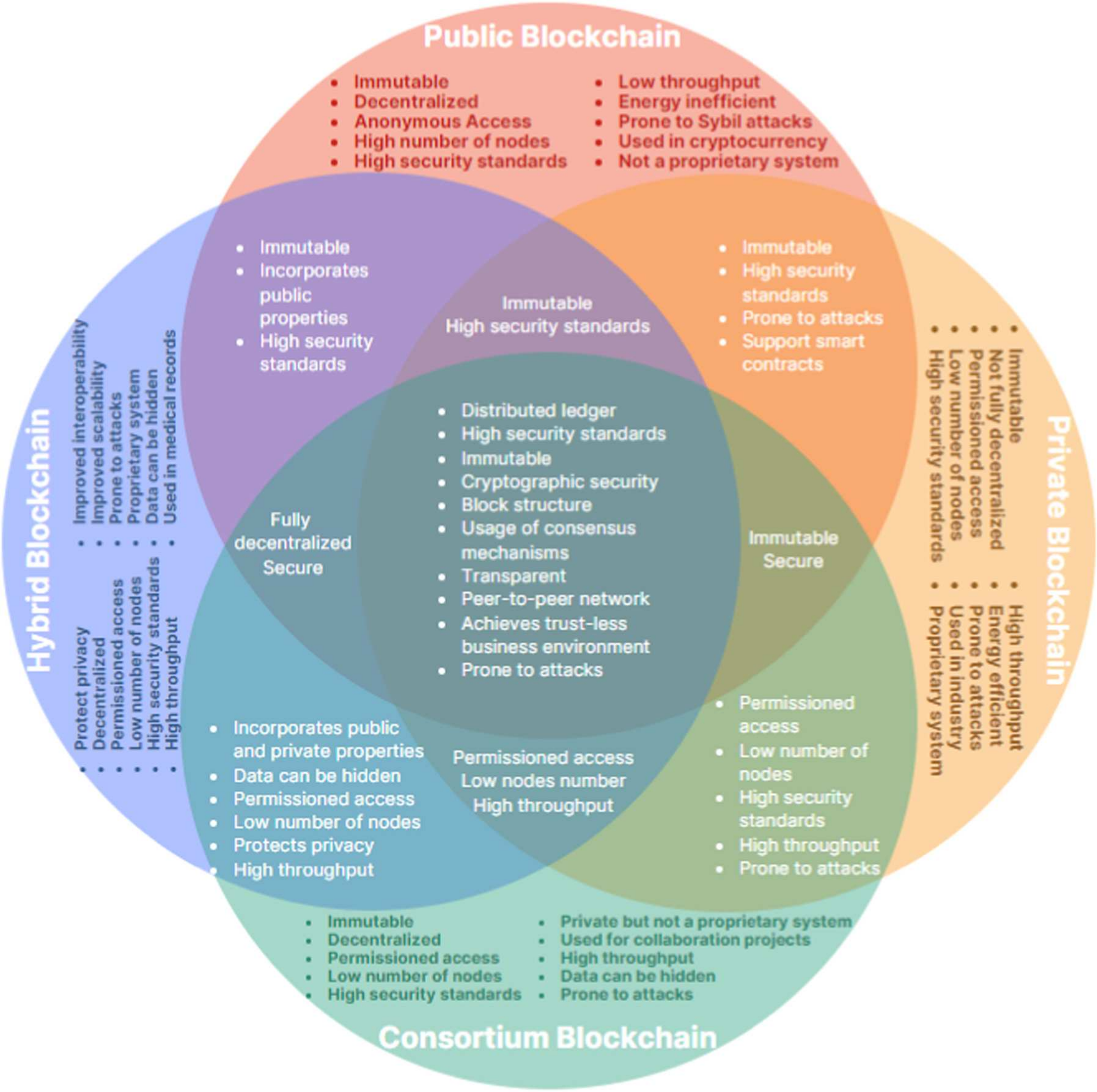


**Fig. 7.** Comparison of blockchain types: public, private, hybrid and consortium.

that more than half of the nodes contributing to the network are not operated by a malicious party and they are honest nodes. Fig. 8 provides a simplistic demonstration of how this algorithm performs.

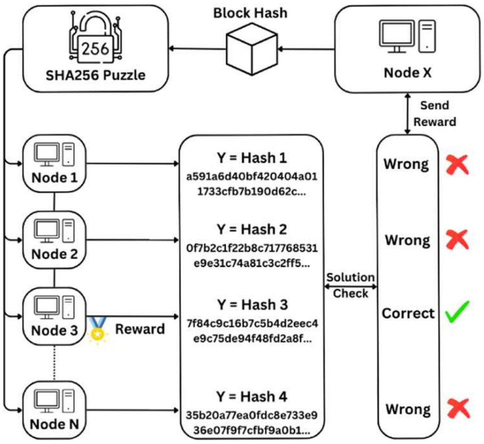

256
SHA256 Puzzle
Block Hash
Node X
Send Reward
Node 1
Node 2
Node 3
Node N
Reward
Y = Hash 1
a591a6d40bf420404a01 1733cfb7b190d62c...
Y = Hash 2
0f7b2c1f22b8c717768531 e9e31c74a81c3c2ff5...
Y = Hash 3
7f84c9c16b7c5b4d2eec4 e9c75de94f48fd2a8f...
Y = Hash 4
35b20a77ea0fdc8e733e9 36e07f9f7cfbf9a0b1...
Solution Check
Wrong ✗
Wrong ✗
Correct ✓
Wrong ✗

**Fig. 8.** Overview of the proof of work (PoW) algorithm.

### 4.1.2. *Proof of stake (PoS)*

In contrast to PoW, Proof-of-Stake (PoS) is an algorithm that selects the miner or node responsible for authenticating a block based on their possession of coins, with those holding more coins and older versions having a greater likelihood of being chosen [49]. During block mining in Proof of Stake, a node’s possession is seized and locked to prevent illegitimate actions. If any such actions occur, penalties are applied and taken from the locked coins. If the addition of a block happens without any suspicious activity, a fee is added to the transaction and the locked coins are released to the original owner and the coin-age value become zero [50]. Although this method is as secure as Proof of Work, it is faster and less resource dependent. However, it is still vulnerable to a 51 % or Sybil attack, although the probability of a node owning 51 % or more of the network is significantly low, thus reducing the risk of such an attack. Additionally, the likelihood of a single party owning 51 % or more of the computational power is low as well. Furthermore, if a party owns a significant share of a network and issues an attack, it will ultimately harm their interests [51]. Fig. 9 represents a fundamental demonstration of how PoS operates. In summary, Proof of Stake is still susceptible to 51 % attacks, but its benefit over Proof of Work is its low energy requirements.

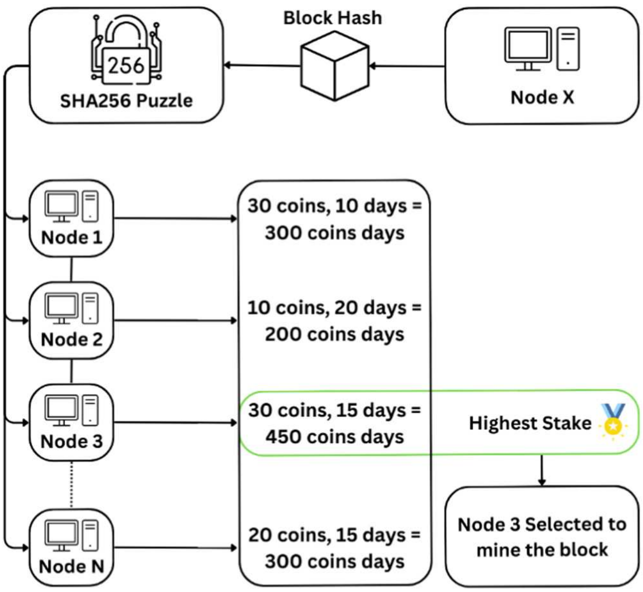

Block Hash
256
SHA256 Puzzle
Node X
Node 1
Node 2
Node 3
Node N
30 coins, 10 days = 300 coins days
10 coins, 20 days = 200 coins days
30 coins, 15 days = 450 coins days
Highest Stake
20 coins, 15 days = 300 coins days
Node 3 Selected to mine the block

**Fig. 9.** Overview of the proof of stake (PoS) algorithm.

### 4.1.3. *Proof of activity (PoA)*

Proof of Activity is a hybrid consensus algorithm that combines the features of PoW and PoS. During the initial phase of validation, PoA operates like PoW. After the first phase is completed, the algorithm switches to PoS to perform a secondary layer of validation [52]. In PoA, the validation process combines elements from both PoW and PoS. During the first phase, all validators, also called miners, are required to solve a complex computational problem that is both time-consuming and resource intensive. While the PoW layer provides an added layer of security, it is vulnerable to a Sybil attack. Once the problem is solved and the block is validated using PoW, it is broadcasted to the network. In the next step, a predetermined number of validators are selected based on their possession, as in the PoS algorithm. These validators then sequentially validate the block or transaction until it reaches the final validator, who is responsible for hashing or encrypting the block and publishing it to the blockchain. By combining PoW and PoS, Proof of Activity (PoA) offers an extra layer of security that reduces the probability of a 51 % attack to almost zero, since the cost of attack is much higher in PoA [53]. Additionally, it promotes security and safety, reduces the likelihood of Sybil attacks, and offers a fair distribution of rewards, along being more energy efficient [54]. Since this algorithm is a hybrid combination of two well designed algorithms, one that relies on the number of honest nodes and the other relies on the possession of coins to honest nodes, when these algorithms are combined their security is merged as well, creating a robust security framework with a very high attack cost. Fig. 10 represents how this algorithm operate and how it combines PoW and PoS.

### 4.1.4. *Proof of importance (PoI)*

Fig. 11 below visualizes the working framework of PoI. The miners in this algorithm are decided by three different parameters which are more generalized to accommodate for everyone in the network and created equality of opportunity, and if these parameters are in favor of an honest node the network will be secured. PoI is a concept like PoS. It rewards nodes with higher possession in the network with a greater chance of

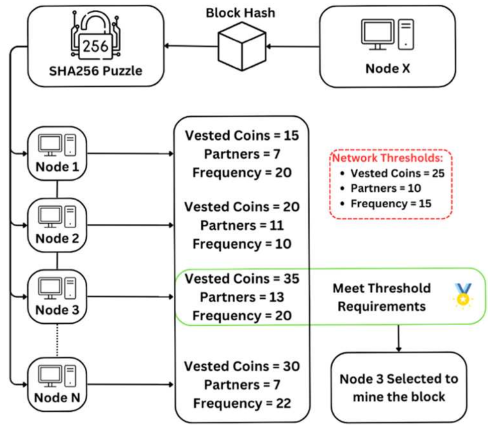


**Fig. 11.** Overview of the proof of importance (PoI) algorithm.

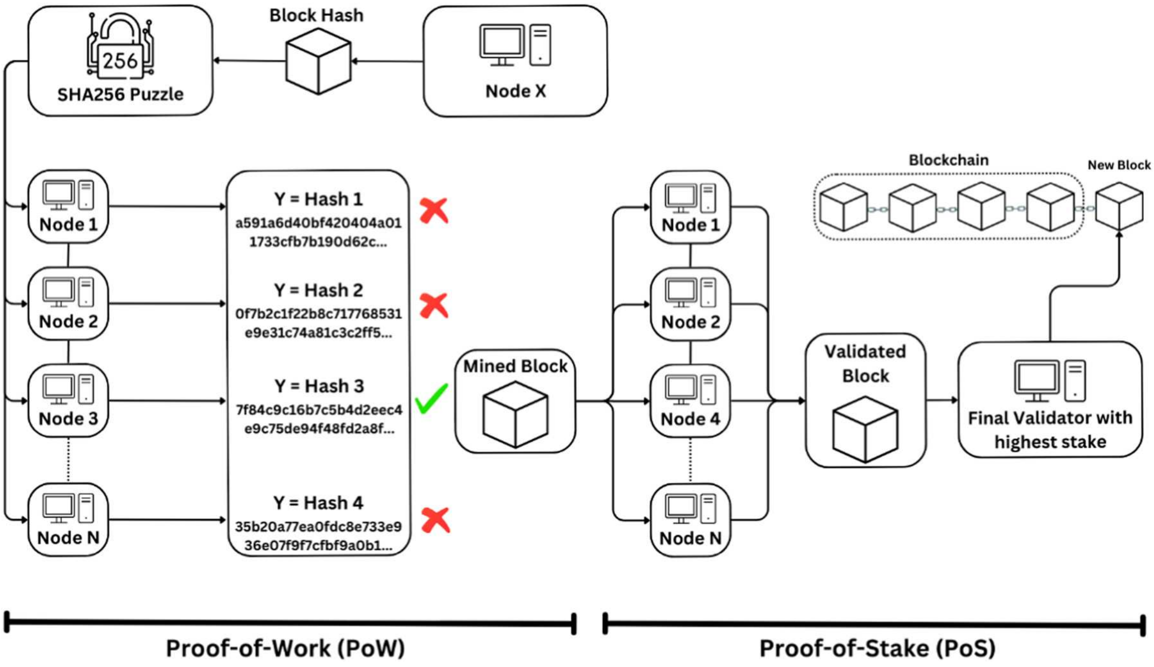


**Fig. 10.** Overview of the proof of activity (PoA) algorithm.

mining new blocks. However, PoS creates a potential imbalance in the system, limiting the opportunities for other nodes to participate and benefit from validating new blocks. In contrast, POI incorporates multiple parameters in the selection process, promoting a more equitable distribution of mining opportunities, even for nodes with relatively lower possessions in the network [55]. The three parameters considered when choosing the validators:

1. Vesting: having a high score is dependent on having a high number of vested coins which are coins that have been in the account for a predetermined number of days [48].
2. Transaction partnership: a node would have a high value of this parameter if it made numerous transactions with other nodes on the network [48].
3. Monthly count and value of transactions: to have a higher score, the transactions made should have an amount above a certain number, and more frequently transactions are made, higher is the score [48].

Differing from PoS, this consensus protocol considers multiple parameters as mentioned previously, which enhances transparency, decentralization, and fairness. Additionally, it is a cost-effective solution, as it does not involve any mining and utilizes minimal resources.

#### *4.1.5. Proof of elapsed time (PoET)*

Proof-of-Elapsed-Time (PoET) protocol was first introduced by Intel in 2016, with the goal of ensuring fairness and equal opportunity for all network nodes to participate in the validation process. Rather than favoring nodes with greater resources or possession, the protocol randomly assigns a wait time to each requesting node, with the node possessing the shortest wait time being selected to validate and publish the block [56]. As a result, PoET offers a fair and energy-efficient alternative to traditional consensus protocols. Fig. 12 explains how PoET operates.

### *4.2. Voting-based consensus algorithms*

#### *4.2.1. Crash fault tolerant (CFT) algorithms*

*4.2.1.1. PAXOS.* The PAXOS algorithm operates in three stages, performed by three classes of operators: proposers, acceptors, and learners [57]. First, one node or a group of nodes serve as proposers and propose a distinct value. Their primary objective is to persuade the acceptors to agree on a single value. Secondly, acceptors, who are the second role in the process, consider the proposals made by the proposers and vote on the value they prefer. After there is a consensus on a value, learners act as the third role and learn the accepted value through majority voting [57]. If the proposer node fails, the acceptors engage in a vote to elect a new leader using the propose-accept procedure [58]. The assumption for the application of PAXOS is that the crashes are not Byzantine faults [57] which are faults that does not rise from hardware or software issues but rather from a malicious attack, byzantine faults are described and discussed in more details in the next section. Fig. 13 represents a demonstration of a PAXOS algorithm reaching consensus, many scenarios could occur for the consensus to be compromised, first and most importantly, if more than 51 % of the nodes fails to communicate, the network will not be able to reach a consensus. Similarly, if the proposer node fails, another proposer will be elected as described before.

*4.2.1.2. RAFT.* The RAFT consensus algorithm was designed to create a simpler mechanism for consensus. In RAFT, all nodes aim to agree on a single leader who obtains most votes. The leader sends heartbeat messages to the followers to let them know of its existence, but communication only goes one way with followers only responding to requests from the leader. If the leader crashes or fails to send heartbeats, followers initiate a new leader election process after a certain period [59]. It is concluded from this algorithm that the nodes blindly follow the leader which makes it intolerant to Byzantine faults because if the leader happens to be a dishonest node, it can induce wrong or malicious information to the system. Fig. 14 represents a demonstration of how RAFT reach consensus, the algorithm is simple and straightforward, however, this mechanism does not tolerate Byzantine fault, it is only resistant to crash faults, and it will keep functioning up until more than 51 % of the network fails.

*4.2.1.3. Apache KAFKA/ KRaft.* KAFKA on its own is a distributed event sharing platform that is used to ensure data consistency and fault tolerance in distributed networks. However, the system on its own is not crash fault tolerant (CFT). KRaft is used as a consensus mechanism that allows data synchronization for Kafka [60] rendering it crash tolerant. Kafka is a relatively new protocol, the architecture of this platform is composed of three hierarchies: Producers, Brokers, and Consumers. First, the type of specific messages is defined by a topic. On this topic, producers can publish messages that will be recorded to servers called brokers. The consumers subscribe to the topics present on the brokers from where they can pull data [61]. KRaft is the consensus algorithm that is like RAFT, however, it is an optimized version in terms of leader election and consensus processes [62]. The RAFT mechanism elects a leader by selecting random nodes that votes for a leader. Conversely, KRAFT improves this process by making the voting recognized. Thus, when any candidate has the most recognition, it is elected as leader. This makes the process of electing a leader more robust, transparent and reliable [62].

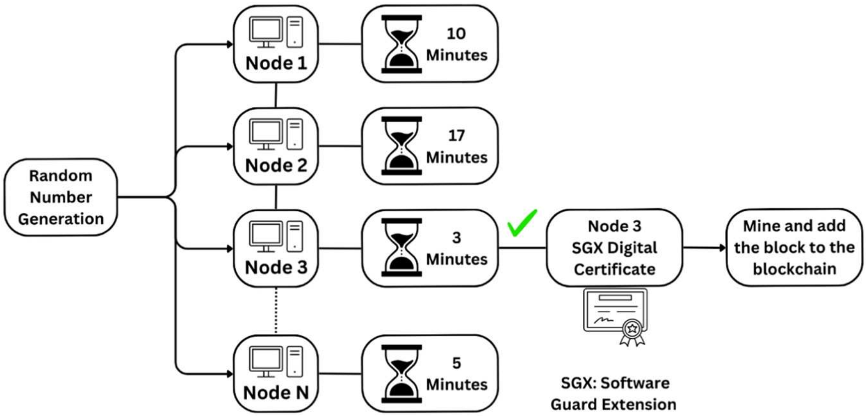

Random Number Generation
Node 1
10 Minutes
Node 2
17 Minutes
Node 3
3 Minutes
Node N
5 Minutes
Node 3 SGX Digital Certificate
Mine and add the block to the blockchain
SGX: Software Guard Extension

**Fig. 12.** Overview of the proof of elapsed time (PoET) algorithm.

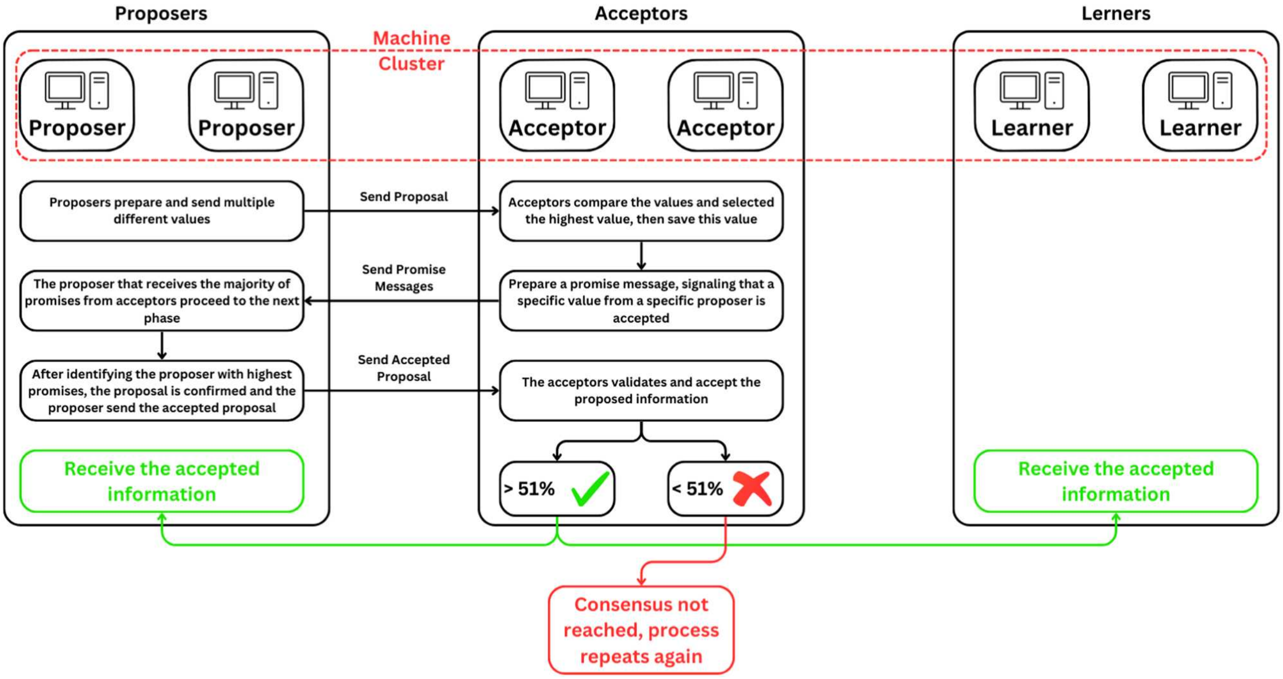

Proposers
Acceptors
Lerners
Machine Cluster
Proposer
Proposer
Acceptor
Acceptor
Learner
Learner
Proposers prepare and send multiple different values
Send Proposal
Acceptors compare the values and selected the highest value, then save this value
The proposer that receives the majority of promises from acceptors proceed to the next phase
Send Promise Messages
Prepare a promise message, signaling that a specific value from a specific proposer is accepted
After identifying the proposer with highest promises, the proposal is confirmed and the proposer send the accepted proposal
Send Accepted Proposal
The acceptors validates and accept the proposed information
Receive the accepted information
> 51%
< 51%
Receive the accepted information
Consensus not reached, process repeats again

**Fig. 13.** Overview of the PAXOS algorithm.

### 4.2.2. *Byzantine fault tolerant (BFT) algorithms*

*4.2.2.1. Byzantine fault tolerance (BFT).* In 1982, Lamport published a paper titled "The Byzantine Generals Problem," which addressed the issue of communication failures and deceit among generals in the Byzantine army. In this scenario, the Byzantine capital was surrounded by enemy forces, and each of the military camps was commanded by a general who could issue one of two orders: to attack or to retreat [63].

This opens the discussion on what are the possible outcomes of such a collaboration knowing that the city is colossal, and the generals cannot directly communicate to have a consensus over a unified decision. In addition, if the decisions of generals are not harmonic, this can result in losing control over the system which is, in this case, the city of Byzantine. After each general takes their final decision, their orders are delivered via messengers to other generals, implying that each general sends their own decision for all the other generals and receives the orders of their fellows.

The interpretation of the situation is assessed under the assumption that all the messengers are honest and will deliver the orders without tampering with the content of the messages. However, throughout history, the presence of traitor generals is common, which drastically increases the complexity of the decision-making and the extent of the success of the defense mechanism.

This problem can be translated into the blockchain world. In blockchain, the database is decentralized and shared between the nodes existing on this network. Specifically, if the blockchain is public, all the nodes can participate in the operation of confirming the authenticity of new information introduced to the system. That leads back to the problem of the disloyalty of certain nodes, which can be thought of as the generals in the Byzantine problem. For the system to be stable and breach-proof, a consensus should be reached in a way to undermine the effect of traitors in the network.

In other words, the system should be able to tolerate the Byzantine problem. The types of failures that are common in public blockchains are classified as Crash Faults, network Faults, or Byzantine Faults nodes. Crash faults are due to different causes from the inability of the node to connect to the network or a malfunction in the hardware where the node does not behave maliciously before it disconnects of after it reconnects [64]. Yet if that type of fault occurs, it stops communicating with other nodes, and its operation is seized but that will not result in detrimental effects, instead, the information traded to or with that node will be delayed, or in the worst-case scenario lost.

The serious threat comes from the crashes that are considered byzantine faults. These nodes send corrupt information to the other nodes, which compensates for the procedure to reach a consensus. In the case of Byzantine Faults Tolerance, to ensure that the network is secured, it is required that less than (N/3) are faulty nodes implying that the percentage of Byzantine faults should be less than 33.33 % out of all the nodes in the network. For more information refer to [65].

In the example presented above (Fig. 15 and Table 1), it is clear how a single treacherous messenger compromised the consensus of all the generals. Here the assumption is that the messages are instantly delivered, but practically in networks over the internet, the case is that the communication is asynchronous which makes the problem even more complex to rectify. The assumption in this example was that the communication is instantaneous and if a general receives two attack orders they will initiate an attack but if they receive a retreat note they will retreat.

*4.2.2.2. Practical byzantine fault tolerance (PBFT).* The initial proposal of the practical Byzantine fault tolerance model was presented by Castro and Liskov in 1999. This model operates in an asynchronous system where participants communicate through a network. In such a network, various failure scenarios may occur, including message delivery failure, delayed information reception, message duplication, or transmission of information out of chronological order [66]. Proof-based consensus algorithms, such as Proof of Work, necessitate that the proportion of malicious nodes in a network is below 51 % of the total nodes or computational power to ensure security and establish a resilient system. In contrast, the Practical Byzantine Fault Tolerance algorithm requires a percentage below 33 % to attain a secure network $\frac{N-1}{3}$ [67]. The notable advantage of employing this algorithm is its low energy consumption and reduced complexity, rendering it particularly suitable for implementation in private or consortium blockchains [68]. The algorithm goes through five steps to reach consensus; *Propose, Pre-prepare, Prepare, Commit, and Reply*.

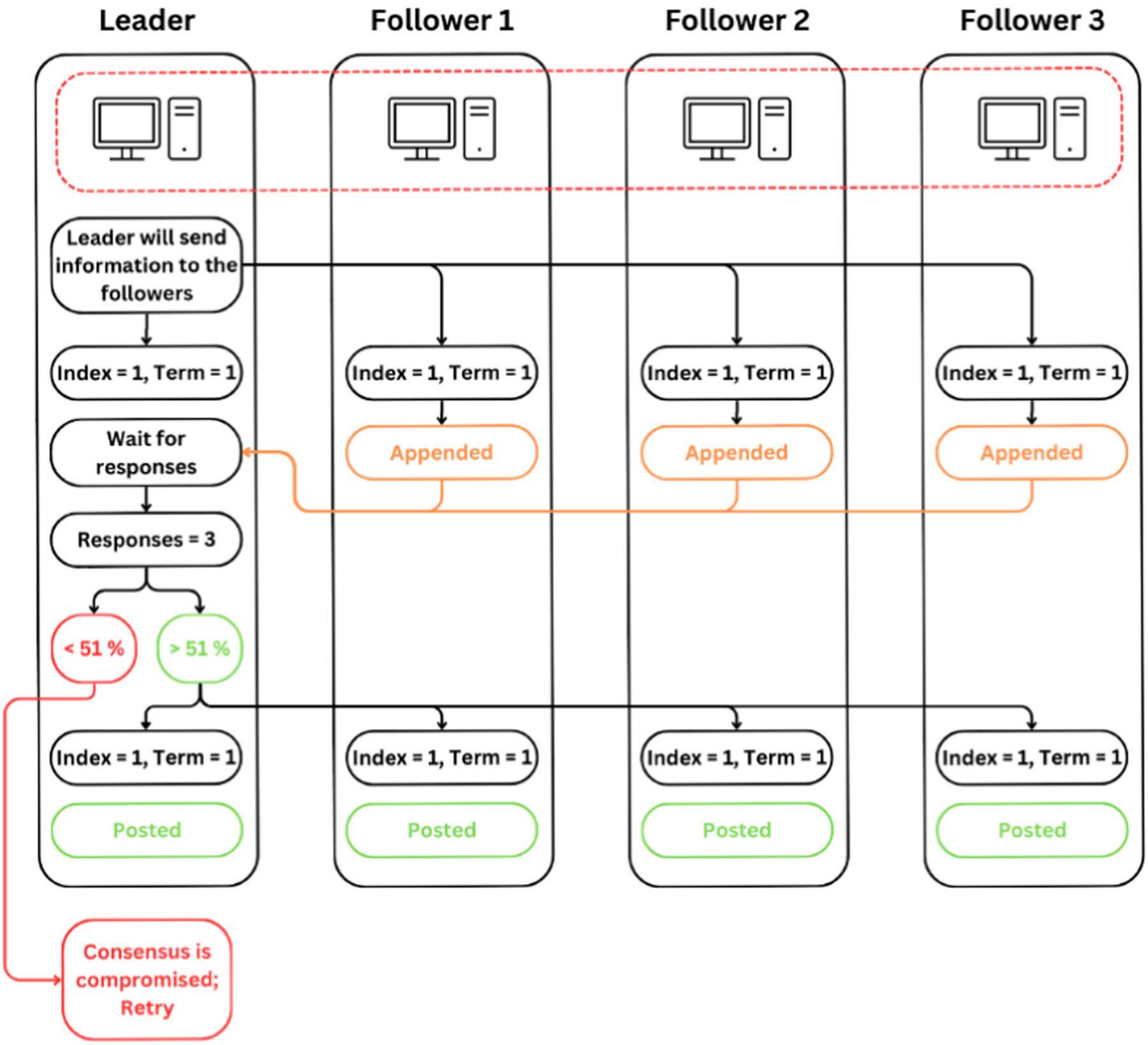


**Fig. 14.** Overview of the RAFT algorithm.

a. Propose: a client publishes a request message to the primary node and replicas.
b. Pre-prepare: the primary node processes the message, adds a sequence number, and generates a pre-prepare message which includes a hash function. A variable reflecting the state at that instance is recorded; if the primary node changes, this value increments by one. The message is signed by the sender using its private key. The primary node then publishes the message to the network, and the replicas receive the pre-prepared message.
c. Prepare: when the message reaches the replica nodes, they verify its authenticity by checking the hash function and validating the originality of the message. Once validation is complete, the replicas generate a prepared certificate and publish the message to the entire network. This occurs only if the number of valid messages received by the replicas is greater than or equal to (2 N + 1). If this condition is met, the system is ready to proceed to the next phase.
d. Commit: The condition for this phase is that the replicas receive (2 N + 1) prepared certificates. If met, the replicas generate a commit message to the rest of the network, and the message is included in the local processing log. The second condition is that the replicas receive (2 N + 1) valid commit messages. If this condition is met, the replicas generate committed certificates, indicating that the message is committed.
e. Reply: in this phase, when the nodes receive (2 N + 1) authentic commit messages from the replicas, the node replies to the client by sending a committed certificate [67].

The following graphic (Fig. 16) illustrates the process described above.

*4.2.2.3. Delegated byzantine fault tolerance (DBFT).* DBFT was designed to facilitate the scalability and performance of Blockchain. In this algorithm, the nodes are divided into groups, and each group votes for a node to be the delegate. The delegates are the nodes that operate together to reach a consensus, the verification of the blocks is made by other nodes. One of the delegates is the leader which serves as the decision-maker. To address more potential problems in such networks, if a delegate behaves maliciously, the group which is led by this delegate can agree to elect a new delegate. In addition, the validation of a block is done by the delegates having enough resources, if these delegates disrupt the process of validation, they are prone to lose their resources. Otherwise, if they behave properly, they are rewarded. In addition, if less than a third of the delegates agree with the leader, it can be replaced. In this fashion, the ability to breach or manipulation resulting from delegate, or leaders are addressed [8]. The workflow of this method is as follows: First, the client sends a request to all the other nodes. Second, one of the nodes which is the primary node sends requests to the other nodes. Third, each node sends its response to all other

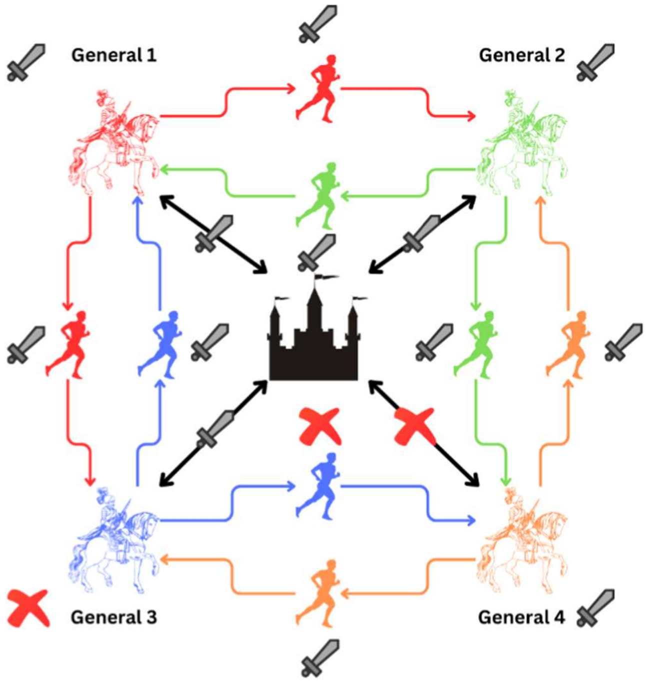


**Fig. 15.** Byzantine generals problem overview.

**Table 1**
Byzantine Generals Problem Decision Table.

| | Initial Decision | Messenger 1 | Messenger 2 | Final Decision |
|---|---|---|---|---|
| General 1 | Attack | Attack (Faulty) | Attack | Attack |
| General 2 | Attack | Attack | Attack | Attack |
| General 3 | Retreat | Attack | Attack | Attack |
| General 4 | Attack | Attack | Retreat | Retreat |

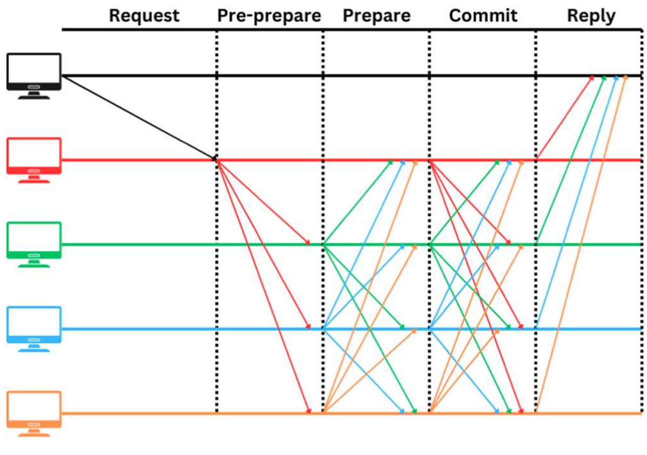


**Fig. 16.** Overview of the practical byzantine fault tolerance (PBFT) algorithm.

nodes. Finally, all nodes send their final response to the client. The process is repeated while delegating a new primary node [69]. To ensure a breach-proof network using this algorithm the number of faulty nodes should not exceed, $\frac{N-1}{3}$. N being the total number of nodes in the network. Fig. 17 describes the process described above.

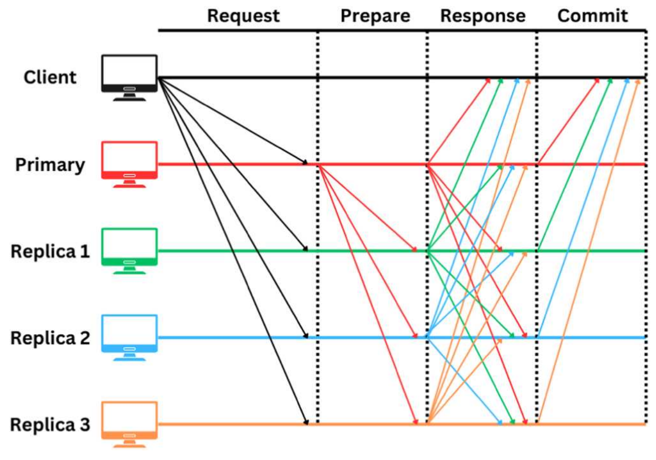


**Fig. 17.** Overview of the delegated byzantine fault tolerance (DBFT) algorithm.

Figs. 18 and 19 classify the consensus algorithms discussed in Section 3. Fig. 18 organizes these algorithms into two categories: Crash Fault Tolerance (CFT), which handles faults arising from software or hardware malfunctions but does not address cyber-attacks, and Byzantine Fault Tolerance (BFT), which can tolerate faults caused by software, hardware, or malicious behavior. Fig. 19 further classifies these algorithms into Proof-Based and Voting-Based approaches.

Table 2 below summarizes the discussed consensus algorithms and represents some of their properties, facilitating the understanding and comparison of these algorithms.

| | Consensus Type | Fault Type | Fault Tolerance | Network | Energy Efficient | Use Cases |
|---|---|---|---|---|---|---|
| PoW | Proof-Based | BFT | $\frac{N-1}{2}$ | Public | No | Bitcoin |
| PoS | Proof-Based | BFT | $\frac{N-1}{2}$ | Public | Yes | Ethereum |
| PoA | Proof-Based | BFT | $\frac{N-1}{2}$ | Public | No | Decred |
| PoI | Proof-Based | BFT | $\frac{N-1}{2}$ | Public | Yes | NEM |
| PoET | Proof-Based | BFT | $\frac{N-1}{2}$ | Public | Yes | Hyperledger Fabric |
| PAXOS | Voting-Based | CFT | $\frac{N-1}{2}$ | Private | Yes | Zookeeper |
| RAFT | Voting-Based | CFT | $\frac{N-1}{2}$ | Private | Yes | Quorum |
| KAFKA | Voting-Based | CFT | $\frac{N-1}{2}$ | Private | Yes | Hyperledger Fabric |
| BFT | Voting-Based | BFT | $\frac{N-1}{3}$ | Pub/Priv | Yes | R3 Corda |
| PBFT | Voting-Based | BFT | $\frac{N-1}{3}$ | Pub/Priv | Yes | HF |
| DBFT | Voting-Based | BFT | $\frac{N-1}{3}$ | Pub/Priv | Yes | NEO |

N represents the number of faults that the algorithm can tolerate, for example, if a network have 20 nodes, the PAXOS will be able to tolerate 9 faulty nodes.

Fig. 20 represents an overview of blockchain systems.

## 5. Discussion on blockchain technology in manufacturing

Blockchain is a relatively new and emerging technology. Despite the numerous benefits it offers, there are limitations and hurdles that impede its widespread adoption. Before applying this technology to any sector or industry, it is crucial to first understand these limitations. This understanding allows for attempts to rectify these issues and assess the technology's suitability, ensuring that the application can accommodate such limitations, this section aims to tackle the prominent limitations that blockchain faces within its intrinsic properties, four hurdles are presented: scalability, interoperability, limitations in the consensus algorithms, and personal sensitive information protection.

### 5.1. Intrinsic limitations in blockchain systems

#### 5.1.1. Scalability

The widespread adoption of blockchain technology in the

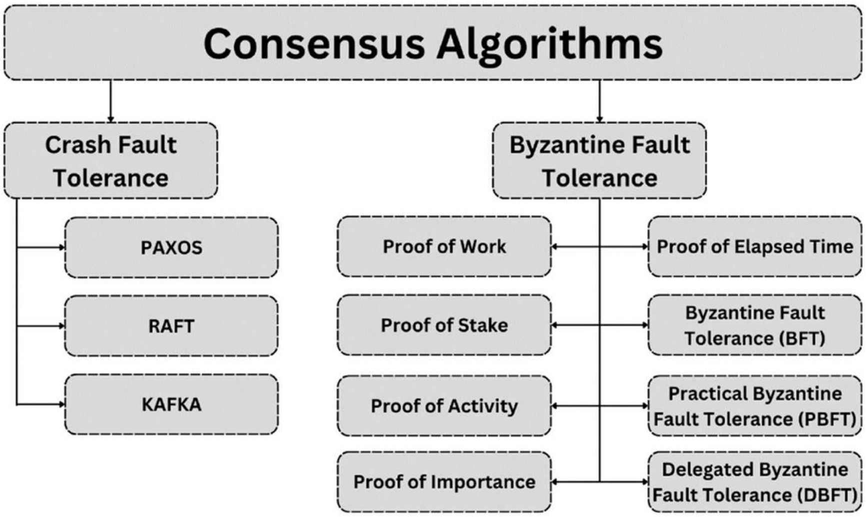

Consensus Algorithms
Crash Fault Tolerance
Byzantine Fault Tolerance
PAXOS
RAFT
KAFKA
Proof of Work
Proof of Stake
Proof of Activity
Proof of Importance
Proof of Elapsed Time
Byzantine Fault Tolerance (BFT)
Practical Byzantine Fault Tolerance (PBFT)
Delegated Byzantine Fault Tolerance (DBFT)

**Fig. 18.** Classification of consensus algorithms: crash fault tolerance (CFT) vs. byzantine fault tolerance (BFT).

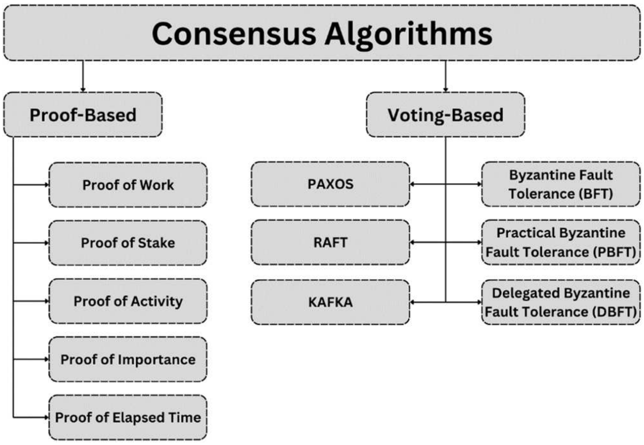


**Fig. 19.** Classification of consensus algorithms: proof-based vs. voting based.

manufacturing industry depends heavily on its reliability, speed, and real-time processing capabilities. As the industry continues to expand with an increasing number of machines, controllers, and sensors, the volume of data being generated is also growing rapidly. Therefore, any system implemented in manufacturing must be both flexible and scalable to keep pace with the industry's ongoing expansion.

Blockchain systems offer a wide range of benefits, however, scalability emerges as a major challenge to the widespread adoption of blockchain in some sectors [70]. The challenge in addressing scalability issues lies in the difficulty of doing so without compromising one or more of the core pillars of blockchain: Security, Decentralization, or Trust [71]. Scalability emerges as a significant issue within blockchain systems as the volume of data transactions continues to grow. Existing blockchain models face limitations in terms of processing speed and capacity.

Consequently, addressing the scalability challenge while preserving decentralization poses an ongoing and formidable task in the realm of blockchain technology [11]. [72] discussed five methods for addressing scalability issues in blockchain: On-chain, Off-chain, Side-chain, Child-chain, and Inter-chain solutions. While each method addresses part of the problem, they also compromise one or more of the fundamental properties of blockchain. Consequently, scalability remains a significant challenge for blockchain technology and requires ongoing research and development to achieve a scalable solution that supports widespread adoption.

### 5.1.2. *Interoperability*

The realm of Smart Manufacturing emphasizes collaboration between facilities, enabling a seamless workflow and simplifying the manufacturing process. Given the variety of blockchain architectures and platforms, it is crucial for this technology to be interoperable when different facilities utilize different platforms and architectures. This interoperability is essential to facilitate effective communication and collaboration across the manufacturing process.

In the previous section scalability was discussed which represents the vertical dimension of blockchain referring to the ability of the system to handle increased load and data processing. Additionally, interoperability represents the horizontal dimension of blockchain pertaining to the capacity of diverse blockchain systems to seamlessly interact and exchange data without the need for intermediary software that translates information to conform to different blockchain platforms. Interoperability represents another major challenge that impedes the widespread adoption of blockchain technology since the majority of existing blockchain systems operate in isolation, lacking the ability to communicate or share data with other systems. Consequently, addressing this significant gap necessitates the development of standardized protocols and frameworks that facilitate interoperability, thus enabling enhanced collaboration and integration among various blockchain networks [73]. Fig. 21 visualizes the description of scalability and interoperability as vertical and horizontal dimensions.

**Table 2**
Blockchain architectures comparison.

| | Security | Energy Consumption | Privacy | Throughput | Complexity | Total Score |
|---|---|---|---|---|---|---|
| Public | Very High (4) | Very High (1) | Low (1) | Low (1) | Very High (1) | 8 |
| Private | High (3) | Low (4) | Very High (4) | Very High (4) | Moderate (3) | 18 |
| Hybrid | Very High (4) | High (2) | Very High (4) | Very High (4) | High (2) | 16 |
| Consortium | High (3) | Moderate (3) | Very High (4) | High (3) | High (2) | 15 |

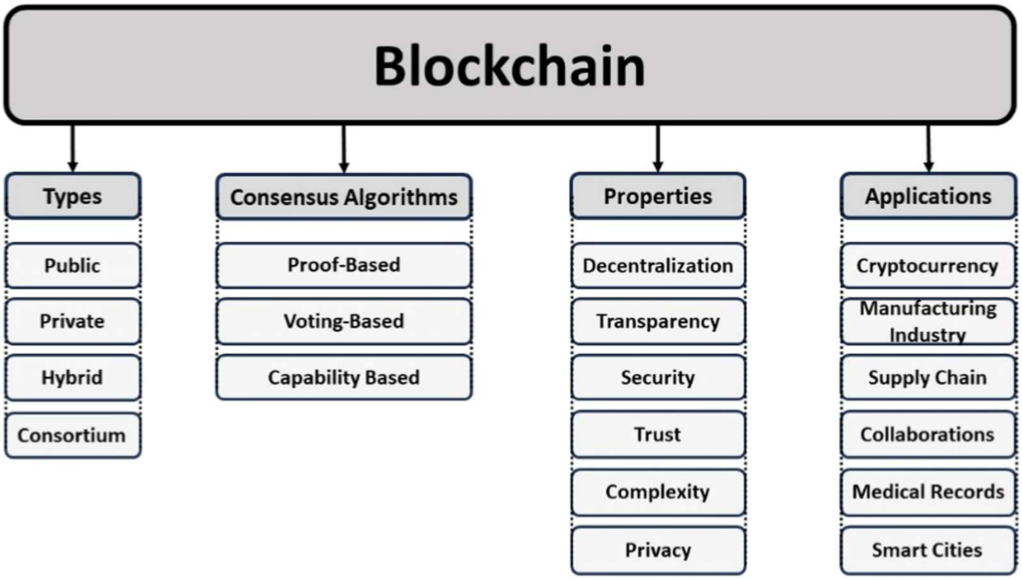


**Fig. 20.** Blockchain systems overview.

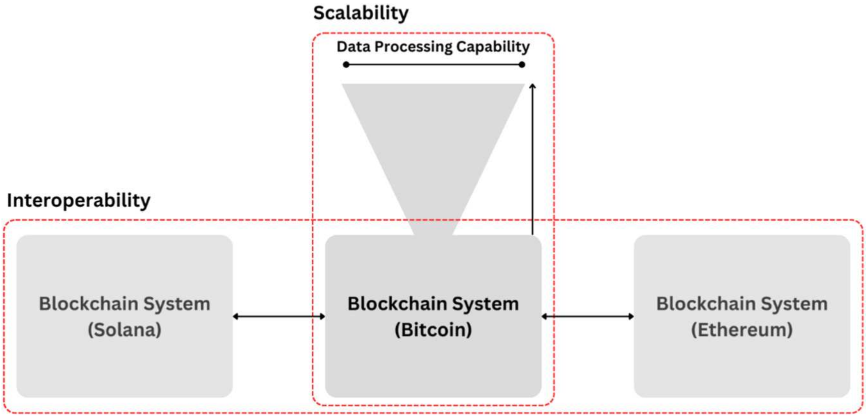

Scalability
Data Processing Capability
Interoperability
Blockchain System (Solana)
Blockchain System (Bitcoin)
Blockchain System (Ethereum)

**Fig. 21.** Scalability and interoperability: a vertical and horizontal perspective.

### 5.1.3. Limitations in the consensus algorithms

Despite the well-developed nature of decision-making algorithms, commonly referred to as consensus mechanisms, it is evident from section three of this paper that each of the currently employed mechanisms possesses limitations, such as the maximum tolerable percentage of faulty nodes in the network, if that percentage is surpassed the mechanism will collapse and security is not guarantee. This may cause the occurrence of majority or 51 % attacks on the network [74].

Section three examined various consensus algorithms, highlighting the diverse approaches available. It is clear that each consensus mechanism currently in use has its limitations. For example, the Proof of Work (PoW) algorithm provides a high level of security but requires substantial energy consumption to maintain that security. Conversely, Proof of Stake (PoS) offers comparable security with significantly lower power requirements, but it risks centralization, as nodes with the largest stakes have more influence over the network. This trade-off between security, energy consumption, and centralization applies to all the consensus algorithms discussed, where addressing one limitation often comes at the expense of another property.

In addition, different types of networks require different types of consensus mechanisms, thus a universal algorithm is not yet developed to suit any type of network seamlessly. These limitations restrict their applicability across all scenarios. Therefore, the development of an efficient consensus mechanism holds paramount importance for ensuring the sustainability of blockchain systems.

### 5.1.4. Privacy issues

Blockchain promotes transparency and immutability which are vital aspects of this technology, ensuring privacy and confidentiality of personal information and data poses a significant challenge for these systems.

As discussed in section two, public blockchains maintain an immutable record that is accessible to the public and allow any node of a network to access the information. Consequently, it becomes crucial to establish a mechanism that safeguards privacy within these networks, in addition to addressing other fundamental aspects of blockchain technology [75].

For instance, in applications involving sensitive data, such as personal or contact information, or financial details, privacy concerns can arise. As noted earlier, once data is recorded on the blockchain, it cannot be permanently revoked or removed. Consequently, this data remains public and accessible, potentially exposing it to malicious actors who may exploit it.

The SWOT analysis in section 5.4.1 examines the privacy of confidential data within blockchain systems, using medical records as an example to highlight potential threats. Due to the immutable nature of blockchain databases, any unauthorized breach would result in leaked confidential data, which cannot be deleted and will remain on the system as long as it is operational. Therefore, establishing robust regulations regarding what can be recorded on the blockchain is imperative to prevent such privacy breaches. Additionally, in section 5.4.4 regulation issues is classified as a threat since regulations are usually dictated by centralized nodes which in this case if a centralized node was assigned to provide regulation it will be contradicting one of the fundamental aspects of blockchain: decentralization.

After presenting the intrinsic limitations of blockchain systems, the next step is to identify the gaps and limitations within the manufacturing industry that blockchain has the potential to address and rectify. Manufacturing sectors with these specific gaps were identified, highlighting their importance within manufacturing systems and outlining the challenges they face. Furthermore, the review discusses how blockchain can potentially rectify these gaps and challenges. The sectors identified by the literature review are categorized into two groups. The first group focuses on supply chain and lifecycle management and includes: Supply Chain Management (SCM), Quality Control Management (QCM), Product Lifecycle Management (PLM), and Inventory Management. The second group is centered on advanced technologies and integration and comprises: Cloud Manufacturing (CM) and Industrial Internet of Things (IIoT).

### *5.2. Gaps and challenges in various sectors of the manufacturing industry*

Over the past decade, significant research efforts have been dedicated to exploring the potential applications of blockchain in manufacturing [76]. Initially motivated by its use case in cryptocurrency and electronic transactions, blockchain has been subjected to further exploration in various other fields. As these use cases expand, the scalability of blockchain has emerged as a crucial challenge as mentioned before, impacting the ability to maximize the benefits and outcomes derived from this technology [77].

In this section, gaps in the fundamental aspects of manufacturing systems will be discussed exploring their respective relevance towards the manufacturing industry. Followed by identifying the gaps that these sectors face as improvements and developments occur to the industry. The revolution of smart manufacturing has added challenges and widened some gaps requiring these systems not only to be efficiently operational but also to consider an additional aspect, which is data security. All machinery, controllers, sensors and other devices used in manufacturing are being connected over the internet, exposing them to be prone to cyberattacks and data breaches resulting in substantial damages and loses. Thus, the focus is rescoped towards the challenges and gaps that blockchain technology have the potential to address. The sectors were divided into two groups, the first group is Supply chain and lifecycle management, and the second group is advanced technologies and integration.

#### *5.2.1. Supply chain and lifecycle management*

*5.2.1.1. Supply chain management (SCM).* Supply chain management encompasses the movement of goods, information, and funds, starting from the procurement of raw materials through production and ending with the delivery of the final product to the end user [78]. While a centralized network is sufficient for small-scale SCM operations that serve local areas, the situation becomes more complicated when expanding the business to a global scale. Operating on a centralized network at this level leads to challenges such as difficulties in achieving scalability, security, transparency, and cost control [79].

As depicted in Fig. 22, products undergo a multitude of shipment and transit processes, often traversing various storage facilities and manufacturing locations, particularly in collaborative manufacturing scenarios. Consequently, ensuring product quality becomes highly challenging, as tracing defects back to their source becomes increasingly arduous.

Smart manufacturing has required higher standards for the supply chain. The first is the synchronization of the operation of the supply chain and the second is ensuring the reliability of the supply chain management [80]. Given these considerations, the evaluation of trust mechanisms within the supply chain becomes essential. The existing supply chain management encounters significant challenges in terms of data security. Data is vulnerable to cyberattacks, breaches, insider threats, and counterfeiting, thus tracking and tracing the products becomes arduous, and real-time flow of costs will be lacking. These above-stated shortcomings of the current supply chain management elevate the risks of incurring additional costs. A blockchain-enabled supply chain trust management was proposed that would lead to solving the stated issues that hinder the smooth process of the supply chain [80].

Blockchain technology revolutionizes the operations of supply chains and logistics by providing enhanced security, agility, trust, and transparency. In the context of supply chain applications, the adoption of a permissioned blockchain architecture proves to be advantageous, as it effectively addresses the challenges associated with multi-organization cooperation and collaboration in areas such as supply chain management, logistics, and transactions [81].

The relationship between blockchain and supply chain was described with three major aspects that create blockchain’s value in that use case. The three attributes are shareability, security, and smart capabilities [82].

Shareability is described by using a peer-to-peer network, this means that all the nodes on the network share their information and all the other nodes on the network receive the same information while having the same distributed ledger. The distributed ledger represents one layer of security.

Security is achieved on three levels; the distributed decentralized ledger is one of the three layers of security as mentioned before [83]. Another layer is the cryptographic technology that includes the hashing

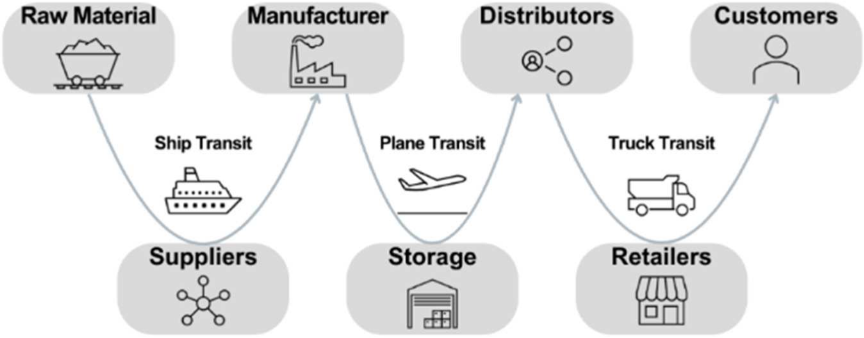


**Fig. 22.** Typical supply chain overview.

of the blocks and relating the consecutive blocks by allowing each block to have its hash and the hash of the previous block, thus creating a blockchain. The third layer of security is the consensus mechanism which provides security for the network overall by ruling all the nodes to abide by a specific algorithm that ensures security [84].

Smart Capabilities in blockchain are the features and functionalities that makes blockchain efficient and versatile, these capabilities include smart contracts, which are self-executing contracts utilizing blockchain technology to digitally enforce, verify the execution of a contract [85].

*5.2.1.2. Quality control management (QCM).* The persistent prevalence of low-quality, defective, and counterfeit products in the market highlights the critical need for a robust quality control management strategy. These issues arise from traditional centralized systems, leading to a lack of trust between parties. In the supply chain domain, these problems stem from the self-interests of supply chain participants, the asymmetric information model in production processes, and the high costs and technical limitations of quality inspection. A decentralized information model, such as blockchain, offers the potential to address these challenges effectively [86].

Quality control management is a crucial aspect across various industries, where the emphasis lies on achieving high-quality production and an efficient supply chain. Blockchain offers a valuable solution in this regard. It enables the establishment of agreed-upon quality metrics, involving clients, manufacturers, and other relevant nodes as participants in the consensus-building process for these metrics. To facilitate the implementation of blockchain, all involved nodes are connected to IoT devices that monitor and provide the required data as specified in the smart contract. The utilization of blockchain ensures the security, authenticity, and tamper-proof nature of the stored data [87]. Moreover, the use of smart contracts enforces responsibility and accountability among the parties involved, thereby enhancing the overall quality control and management practices.

The ability to efficiently track defects that occur within manufacturing processes, along with the capability to trace incorrect handling conditions within supply chain systems, is crucial for identifying the root causes of these problems. Collecting data from various sensors and contextualizing these readings plays a vital role in identifying such defects. However, in centralized systems, this data can be modified to benefit certain parties, for instance, if data indicates that a particular defect resulted from mishandling by a specific party, and this party has access to the centralized data storage, they could potentially alter the data to conceal the defect, thereby avoiding liability. In contrast, blockchain systems are designed so that once data is recorded, it becomes immutable and undeletable. This feature prevents the modification of data to conceal manufacturing or supply chain issues. Additionally, because the data is authenticated, tracing the root cause automatically induces accountability, thereby improving product quality from the manufacturing facility through the entire supply chain. This ensures customers receive untampered, high-quality products.

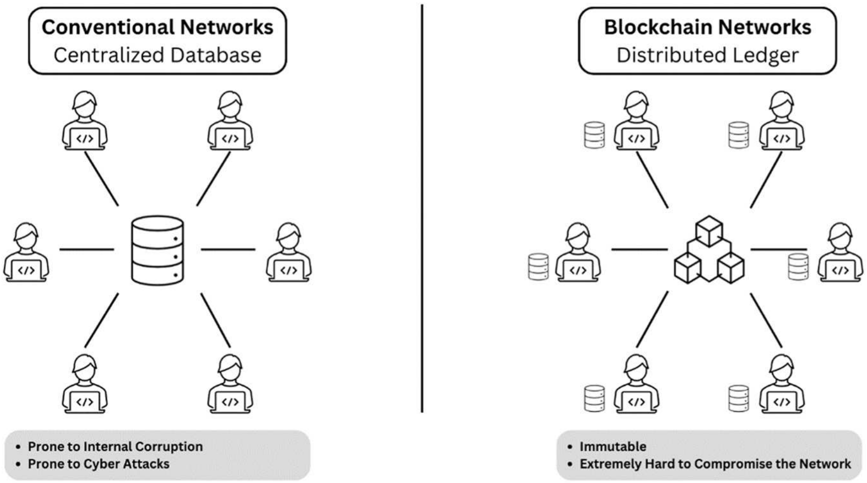
Fig. 23 illustrates the difference between centralized conventional networks typically used in manufacturing systems and the distributed ledger model of blockchain. In centralized systems, there is a single point of failure (SPOF); if the centralized database is breached, the network risks losing all data. In contrast, blockchain systems ensure that each node has a copy of the ledger, which is cryptographically protected and maintained by robust consensus algorithms to ensure consistency across all ledgers. This architecture creates a network resistant to cyberattacks and insider threats.

*5.2.1.3. Product lifecycle management (PLM).* Product Lifecycle Management (PLM) can be categorized into four distinct stages: product design, manufacturing, product usage, and recycling. Each of these phases exhibits certain deficiencies or gaps in their respective processes. In this literature, the focus is directed toward the design and manufacturing phases since these are the realms where defects can manifest. Fig. 24 represents potential errors that could result in the phases that the study is interested in.

**Design Phase:** the design phase holds significant importance as it contributes up to 75 % of the overall cost associated with the products. The design directly affects all the subsequent phases. This stage itself consists of four sub-stages. It encompasses task clarification, conceptual design, embodiment design, and detail design [88]. These design phases encompass numerous key components that directly impact the overall quality of the final product. Ensuring traceable and transparent data throughout these phases promotes accountability, motivating designers to maintain accuracy in these critical manufacturing stages. Additionally, a secure database offers the advantage of preserving design data in its original format. This allows for tracing any mistakes back to their root cause and ensures that design files cannot be altered, providing a reliable reference for future use.

Facilitating a suitable collaborative platform for designers from different entities across the globe can result in optimal designs and well-informed decisions during this crucial phase [89].

Moreover, the availability of a secure repository for storing design documentation ensures data integrity and prevents tampering. This is particularly valuable for preserving copyright protection and enabling traceability of original designs [90]. Significantly, the trustworthiness and authenticity of these documents may allow companies to monetize their design documentation, in many cases the documented designs get



• Prone to Internal Corruption
• Prone to Cyber Attacks
Blockchain Networks
Distributed Ledger
• Immutable
• Extremely Hard to Compromise the Network

**Fig. 23.** Comparison between conventional centralized database vs. blockchain decentralized database.

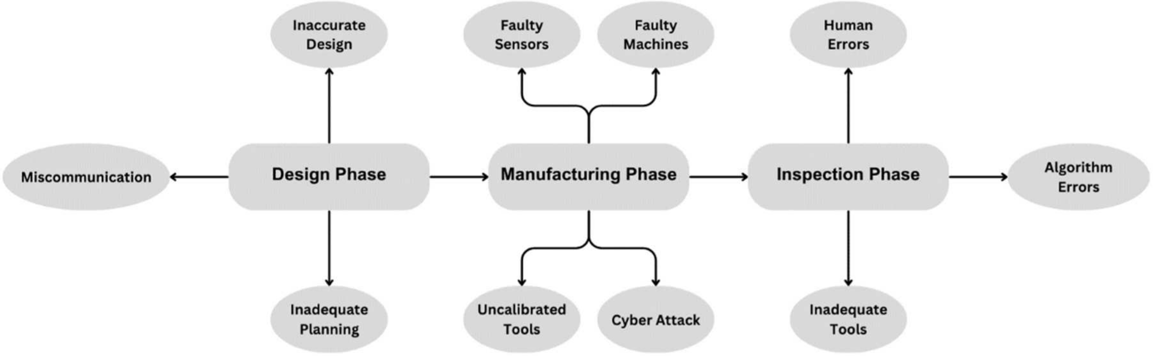


**Fig. 24.** Potential sources of anomalies in manufacturing processes.

lost, corrupted, or mixed up between tens of versions that result in losing the original files, but when the latest designs are stored in a database where blockchain technology is applied, these files cannot be changed nor deleted, thus it is safeguarded, which makes it possible for these companies to sell their designs to other companies with a high level of confidence that the files do not contain any type of errors. Blockchain technology serves as a viable platform for such purposes, distinguished by its secure communication protocols, reliable data exchange, and authentication mechanisms.

**Manufacturing Phase:** In the manufacturing phase, numerous potential errors could compromise the overall quality of the final products. As illustrated in Fig. 24, issues such as faulty sensors or malfunctioning machinery control signals can lead to defects. Blockchain technology can be utilized to store these signals securely, ensuring they cannot be modified to conceal errors, thereby facilitating efficient tracing of the root causes of problems. Additionally, a cyber-attack could disrupt the smooth operation of machinery, resulting in defective products or, in more serious cases, damage to the machinery itself. On the inspection side, human errors can occur, thereby implementing automated inspection methods [91] can significantly reduce the number of errors in the inspection phase, however, automating manufacturing processes requires a secure cyber-physical infrastructure. Implementing blockchain technology can help counter such attacks by employing multiple layers of security. Blockchain can differentiate authentic data from malicious data, allowing only verified data to pass through the controllers and rejecting any potential malicious data aimed at inducing faulty signals to the machinery.

The quality of raw materials emerges as a paramount factor influencing the final outcomes [92]. However, the existing centralized system often favors large suppliers, for example, these suppliers can produce goods at a lower rate than smaller suppliers, and the centralized system favors suppliers with greater negotiation power, thus, leading to market dominance and inhibiting trust and authenticity for smaller suppliers due to prevailing monopolies. As a result, the quality of raw materials can suffer as suppliers prioritize cost reduction and maximize their own benefits.

In contrast, the decentralized nature of blockchain empowers every supplier with equal trust and authority, providing equal exposure to the market regardless of the scale of the supplier, thus fostering a more competitive market environment. Usually, small suppliers are reliant on third parties to be able to access the market, with blockchain applied, this intermediary is omitted since blockchain opens the option for peer-to-peer transactions, reducing the overall cost for small suppliers. In addition, blockchain gives small suppliers the ability to access the global market needless of a physical presence or complex international infrastructure, thus expanding their market reach. This increased competition compels suppliers to deliver the best available products, promoting their competitiveness and survival in the market.

*5.2.1.4. Inventory management.* The management of inventory poses a significant challenge in manufacturing, particularly when dealing with customized orders that involve a diverse range of parts. This complexity is further compounded by the need to efficiently handle inbound logistics for transporting these customized parts from providers to manufacturers. To address this challenge, a potential solution lies in leveraging blockchain applications. By utilizing a blockchain platform, customized orders can be shared and recorded through smart contracts, enabling effective mapping of the required parts. Subsequently, logistics arrangements can be streamlined accordingly. This approach enhances the efficiency and cost-effectiveness of the order customization process, ultimately contributing to improved flexibility in manufacturing operations. Utilizing blockchain technology to improve inventory management and information sharing in the supply chain was demonstrated by [93].

The preceding sections discussed the pivotal role blockchain technology can play across various hierarchies in manufacturing. For instance, in Enterprise Resource Planning (ERP), blockchain can address issues such as inventory management, as highlighted in the previous section. At the Manufacturing Execution System (MES) level, blockchain can help establish a secure and robust cyber-infrastructure, enabling secure manufacturing communication and control. Additionally, within the ERP framework, financial transactions can be executed on blockchain systems without the need for a third-party validator. This facilitates seamless and secure peer-to-peer transactions, reducing budget overheads associated with third-party services, minimizing transaction validation lag time, and maintaining a transparent record of all transactions to ensure comprehensive financial disclosures.

### 5.2.2. Advanced technology and integration

*5.2.2.1. Industrial internet of things (IIoT).* The data exchanged between different entities are obtained by the Industrial Internet of Things (IIoT), which has a high “trust tax” [94]. This means that the communication between the nodes of collaborative projects is based on trust which increases the risks of security issues. When communicating important data, it is extremely important to maintain security, robustness, and authentic data to ensure a secure exchange of confidential data [95].

The rising security challenges that face the implementation of IoT were reviewed by [96], and proposed a framework to secure IoT devices, using the strategy of Zero Trust and blockchain. Counterintuitively, blockchain is commonly associated with a "trusted" network, yet its actual concept revolves around facilitating "trustless" transactions. This means that the various parties involved in the system are not required to trust one another directly. Rather, they place their trust in the system itself, which is designed to provide reliable and trustworthy data. Consequently, blockchain holds promising potential as a solution for enhancing the security of data exchange within the IoT ecosystem. The blockchain features the ability to overcome cybersecurity challenges and apply a high degree of privacy [97]. Blockchain as described before is a shared peer-to-peer network that gets updated every time a change happens. The information on blockchain once recorded is extremely difficult or even impossible to alter or delete [98]. Which is an aspect that fills one of the gaps in IoT systems. A new concept was proposed which is the Blockchain of things (BCoT) that delves into exploring the advantages of mixing IoT and blockchain [99]. One way to implement blockchain to IoT is that the system will make a unified authentication for identities and make list containing the public keys of the users, attributes, and a list that includes the list of revocations [95].

According to the data collected the administrator of the system generates the private keys for users. When these users perform on the network, their attributes should match with the security policies set. In addition, they should not be included in the revocation list, after these authentications users can attribute to the network. Malicious attackers can then be detected and listed on the revoked list; this can take place at any stage. Furthermore, machine learning algorithms can be integrated into this system. Edge computing is a powerful tool for real-time data processing of information in the IIoT. But since the number of edge devices connected to the networks is large and still increasing, this results in privacy and security issues. For this a blockchain-based machine learning framework was proposed for edge services in IIoT [100].

Within extensive industrial facilities, numerous pieces of equipment are dispersed throughout the premises, necessitating effective communication among them. Presently, communication protocols such as Modbus or PROFINET are commonly employed for this purpose. While these protocols offer efficiency, they also entail inherent risks of data corruption or unauthorized access. To mitigate these risks, blockchain applications can be employed, wherein each machine or equipment functions as a node within the network, enabling secure data transmission. By leveraging blockchain technology, the integrity and confidentiality of the transmitted data can be ensured, enhancing the overall security of the communication process.

*5.2.2.2. Cloud manufacturing (CM).* Cloud manufacturing encompasses the utilization of cloud infrastructure for activities such as design, collaboration, and idea sharing. Through the cloud, designers from diverse entities and geographical locations can collaborate on projects. However, due to the public nature of this communication, the risk of security breaches becomes unavoidable. To mitigate these risks, a centralized third party is typically required to validate the data. In contrast, blockchain technology, with its decentralized and distributed nature, offers an alternative approach by ensuring data immutability and establishing trustworthiness [101]. At a different level, cloud manufacturing can involve two entities: providers and consumers. In this scenario, the two parties do not physically meet, and the entire collaboration relies on trust that the data provided by the providers is genuine, non-malicious, and free from corruption [102].

To tackle this challenge, one potential solution is the implementation of a blockchain that guarantees the credibility and authenticity of the data. Facilitating data sharing while ensuring that logs are securely preserved in the database allowing any malicious data to be easily traced back to the entity that provided it. This ensures data authenticity and enhances accountability, which plays a crucial role in maintaining the integrity of the system.

Post identifying these gaps, an additional step was taken to identify a more complete security framework that showcases the inseparable relation between blockchain and cybersecurity. Blockchain technology employs various methods to ensure security, including cryptographic security through hash functions, digital signatures unique to each user, and the Public and Private Key Infrastructure (PKI). Additionally, consensus protocols and encryption for secure data transmission contribute to its robust security standards. These measures create an environment where data cannot be altered or deleted. However, an important question arises: what if the data is corrupted before being recorded into the blockchain? This would undermine the purpose of implementing blockchain. Therefore, the interconnection between blockchain and cybersecurity is crucial, as these two security pillars complement each other to achieve a comprehensive security framework. This interconnection is discussed then a real-life case is presented to showcase the impact of data breaches on the manufacturing industry.

### 5.3. Interconnection between blockchain and cybersecurity

Transparency and immutability are critical features of blockchain technology that play a vital role in ensuring traceability and quality control. These features provide security on the premise that the received data is authentic and remains unaltered. However, further research is required to identify the most effective approaches for receiving and validating data from monitored sources within blockchain systems [103]. It is imperative to delve deeper into the realm of cybersecurity to explore and develop these aspects, enabling stronger data integrity and enhancing the overall security of blockchain implementations.

Fig. 25 illustrates the communication layers from sensors to the storage level, passing through communication channels such as the internet. These channels are crucial for the effective implementation of blockchain. If sensor values are altered within this medium before reaching the blockchain security layers, it compromises the entire security of the blockchain. This would result in the system recording and securing faulty data, thereby defeating the purpose of the implemented system.

In 2022, one of the biggest supply chain cyber-attacks targeted the vehicle manufacturer Toyota which specifically targeted a major component supplier under the name of “Kijima Industries Corporation”. It is suspected that the attack is a ransomware ambush. Although the attack was not officially confirmed, in the due time the manufacturing process was halted. The aftermath of this incident cause Toyota to drop their monthly production by 5 % within Japan which is equivalent to 13000 units monthly [103]. Many other major attacks occurred that caused notable disruptions in the supply chains which resulted in huge financial losses. The depicted Fig. 26 illustrates the complete process of transmitting data from a sensor to its storage in blockchain. The transmission of data holds great significance as blockchain ensures the safety and authenticity of the collected data. Consequently, the authenticity of the data within blockchain relies heavily on the authenticity of the received data. Therefore, cybersecurity assumes a critical role in verifying the authenticity of the data received from sources like the supply chain, and recording it in blockchain in its original, unmodified state.

## 6. Supply chain cyberattacks and breaches

Despite witnessing significant advancements, traditional supply chain systems that have been in use for decades still face a persistent issue of lacking transparency. While data recording and technology utilization are efficient, there remains a vulnerability to data breaches and unauthorized modifications. Unfortunately, such incidents occur frequently, as evidenced by the global average cost of a data breach amounting to USD 4.35 million in 2022, as reported by [104].

As depicted in figure X, the cost associated with data breaches is expected to rise in the coming years. This projection assumes that no preventive measures are implemented to mitigate such attacks and breaches. However, blockchain technology presents a robust solution to combat these threats. Its decentralized nature serves as a deterrent against malicious actors, as it inhibits their ability to manipulate and compromise data. Blockchain systems effectively tackle another challenge within the supply chain, which is the recording of every transaction and event throughout the entire process, starting from raw materials and culminating with the end customer. This enables all participants to have real-time tracking of products and the ability to assess their condition.

As illustrated in Fig. 27, data is exchanged between nodes within the blockchain network, establishing a peer-to-peer network where information is accessible to all participating parties. This decentralized

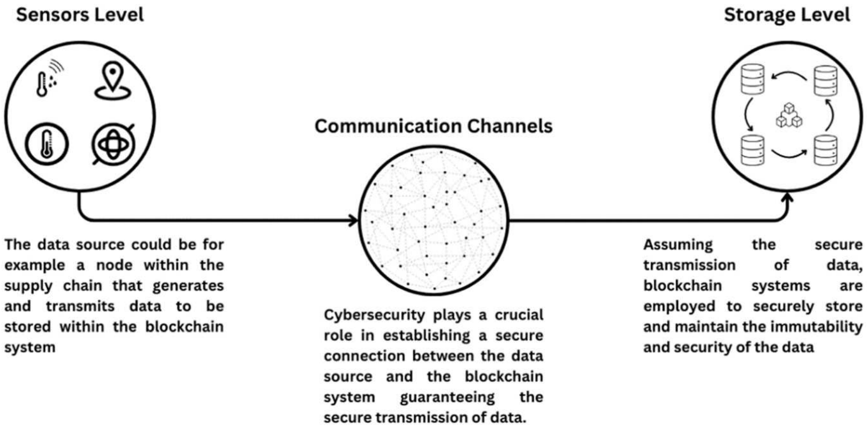

Sensors Level
Communication Channels
Storage Level
The data source could be for example a node within the supply chain that generates and transmits data to be stored within the blockchain system
Cybersecurity plays a crucial role in establishing a secure connection between the data source and the blockchain system guaranteeing the secure transmission of data.
Assuming the secure transmission of data, blockchain systems are employed to securely store and maintain the immutability and security of the data

**Fig. 25.** Synergy between blockchain and cybersecurity.

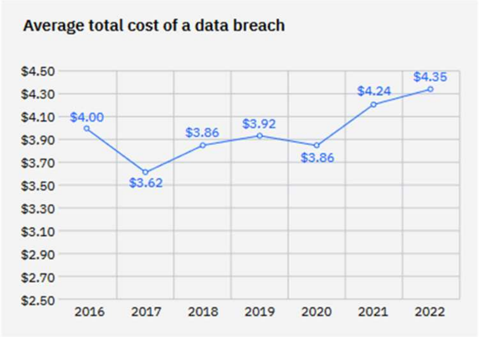


**Fig. 26.** Average total cost of a data breach from 2016 to 2022.

structure enables thorough tracking of each product's history, allowing for the identification of the origin of any defects. Therefore, individuals can be held accountable for any unprofessional actions or mistakes, thereby ensuring a higher level of responsibility and accountability. Furthermore, the manufacturing process is a formidable and intricate process, particularly when dealing with mass production in factories. The complexity stems from the multitude of steps involved, starting from sourcing raw materials to delivering the final product to the end customer. Among the many challenges within this process, effective inventory management stands out as a crucial aspect. Anticipating demand becomes exceptionally difficult due to the multitude of variables that influence this parameter.

Accordingly, inventory management becomes a challenging task. However, with the integration of blockchain into the supply chain, real-time inventory tracking becomes feasible across the entire supply chain network. This ability to track goods as they move from one node to another provides a vital indicator of inventory levels, granting organizations control over one of the numerous parameters that contribute to reducing stockouts and improving demand forecasting. In addition, ensuring the quality control of products is of utmost importance in the production process, particularly when dealing with high-standard and highly regulated items like pharmaceutical products for example. Monitoring various environmental parameters such as temperature, humidity, and other relevant factors throughout the entire supply chain plays a vital role in determining the quality of the final product.

Blockchain systems greatly facilitate this task by offering a secure data storage infrastructure where such critical data can be recorded and preserved without the risk of unauthorized modifications or

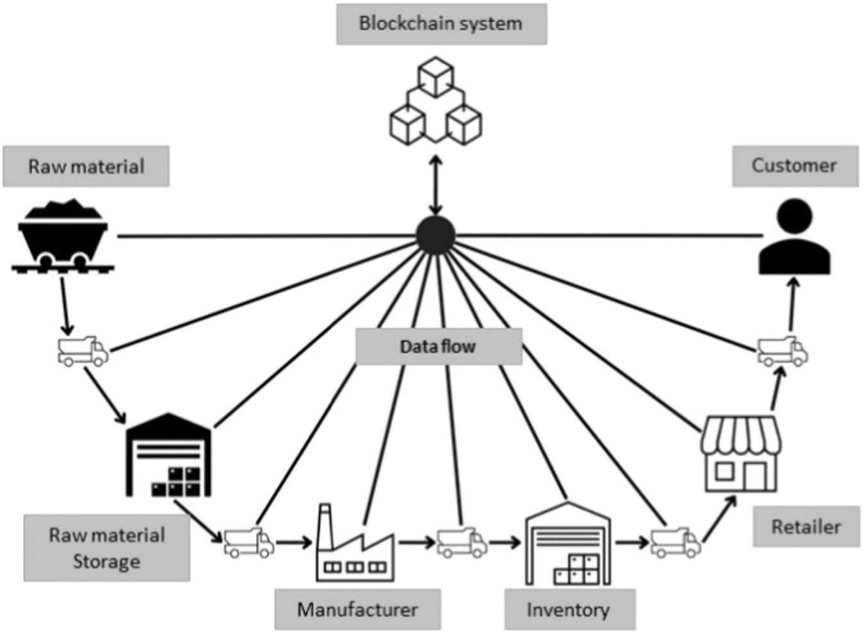


**Fig. 27.** Blockchain application in supply chain management (SCM).

manipulations. This inherent security provided by blockchain technology significantly reduces the risks associated with counterfeiting and fraudulent activities, enhancing the overall integrity and trustworthiness of the supply chain.

On the other hand, transactions and payments pose significant challenges within the supply chain, often consuming time and relying on trust between parties. Instances of delayed or erroneous payments due to human or other errors can further complicate the process. In this regard, blockchain-based smart contracts offer a solution whereby payments can be automatically triggered upon the fulfillment of predefined conditions, such as the confirmation of delivery. This automation of payments has the potential to mitigate delays, minimize paperwork, and eliminate the need for third-party authentication of transactions, such as involvement from banks. By leveraging blockchain, the supply chain ecosystem can benefit from streamlined and more efficient payment processes.

Ultimately, the integration of blockchain technology into supply chains is an active area of research and implementation. Nevertheless, the process of integrating this technology into existing supply chains poses significant challenges. Further research is required to develop efficient methodologies that enhance the seamless integration of blockchain systems and facilitate the exchange of data. Additionally, there is a crucial need to enable real-time tracking within the supply chain through the utilization of blockchain technology. Advancements in these areas will contribute to the effective integration of blockchain into supply chains and enable its full potential to be realized.

## 7. SWOT analysis

Section 2 addressed the categorization of blockchain architectures. The focus of this literature review is on manufacturing systems, aiming to identify key sectors where blockchain technology could address existing gaps and challenges. The goal is to determine the most appropriate blockchain architecture and consensus algorithm for these sectors. As highlighted in the review, supply chain management is critically important across the industry. Enhancing security in the supply chain not only resolves issues within that domain but also positively impacts related areas such as Quality Control Management, Product Lifecycle Management, and Inventory Management, all of which are interconnected through the supply chain. Therefore, addressing supply chain issues can lead to improvements in these related sectors.

Initially, Section 2 explores public blockchains, known for their high security due to the Proof-of-Work (PoW) consensus algorithm. However, PoW is energy-intensive and requires substantial computational resources, as detailed in Section 3. A potential solution is to replace PoW with Proof-of-Stake (PoS) to reduce energy costs. Yet, public blockchains are inherently open, which can pose problems for industries where sensitive information, such as strategic plans, must remain confidential. Moreover, public blockchains have relatively low transaction throughput due to the complex consensus process, and their implementation is complex. Consequently, public blockchains may not be the optimal choice for industrial applications.

In contrast, private blockchains offer a highly secure framework with low energy consumption. They support various consensus algorithms like PAXOS and RAFT, which are resilient to crash faults but not necessarily to malicious attacks. More advanced algorithms, such as PBFT or DBFT, can enhance security against cyber threats, as discussed in Section 3. Private blockchains ensure privacy by restricting network access to approved entities only, thereby safeguarding sensitive data. They also provide high throughput, making them well-suited for real-time data needs in industrial contexts. Additionally, private blockchains are generally less complex to implement than other architectures, making them a strong candidate for manufacturing, especially in supply chain management.

Hybrid blockchains integrate features of both public and private blockchains, potentially improving certain system aspects. However, this integration introduces additional complexity, requiring specialized expertise not commonly found in the manufacturing sector, where the focus may not be on these advanced applications. Additionally, the integration of public properties induces higher energy consumption for this architecture.

Consortium blockchains offer security and other features like private and hybrid blockchains but are decentralized and not owned by a single organization. The implementation of consortium blockchains, like hybrid blockchains, demands specific expertise that may not be readily available in the industry. Additionally, complete decentralization comes at the expense of higher energy consumption for this architecture.

In summary, private blockchains are highly suitable for manufacturing applications, especially in supply chain management, due to their security, efficiency, and lower complexity. While hybrid and consortium blockchains offer certain advantages, they introduce additional complexity and require specialized knowledge on top of higher energy consumption.

The following table summarizes the comparison to help quantify the advantages and disadvantages of each blockchain architecture, aiding in the identification of the most suitable option for manufacturing industries. The scores were assigned based on four levels: Low, Moderate, High, and Very High. For properties with a positive contribution, Very High was given a score of 4, and Low a score of 1. Conversely, for properties with a negative impact, Very High was scored as 1, and Low as 4. These quantifications were derived from the conclusions of the information gathered in this literature review.

After quantifying the scores of the different blockchain architectures, private blockchain architecture proves to be the most suitable for manufacturing industry. Although hybrid and consortium have high scores as well, their energy consumption and complexity to be implemented favors private blockchain for these applications. Subsequently, in Section 5, a thorough SWOT analysis was conducted for this specific blockchain architecture.

### 7.1. Strengths

#### 7.1.1. Decentralized

Private blockchain operates on a peer-to-peer network, eliminating the need for a third-party organization to manage the database. Instead, each node in the network maintains a copy of the ledger, which is updated through a consensus algorithm. The nodes communicate directly with each other, ensuring there is no centralized node [105]. The importance of this feature is that it eliminates the presence of a single point of failure (SPOF) in the system. In centralized systems, if the central node is compromised, the entire system can fail. However, in blockchain networks, the system can continue to operate normally as long as a specific percentage of nodes remain functional, the percentage is specified by the consensus algorithm used. This makes breaches significantly more complex and harder to successfully achieve.

#### 7.1.2. Immutable

The cryptographic security of data and the distribution of ledgers ensure that once a block is added to the blockchain, it cannot be altered or deleted. This feature, referred to as immutability, guarantees the integrity of the data recorded on the blockchain and prevents any unauthorized changes to the information [106].

#### 7.1.3. Transparent

Because of the decentralized nature of blockchain, the database is shared among various nodes in the network, which allows for transparency in information sharing. This transparency is further enhanced by the chronological order in which data is recorded on the blockchain, making it useful in tracking specific information in the supply chain [107] for example. Transparency is crucial in private sectors, such as the manufacturing industry, because it fosters trust between entities. Additionally, it enhances the traceability of data, which ultimately improves accountability and responsibility—two essential features, especially in supply chain management.

#### 7.1.4. Secure

The fundamental strength of blockchain lies in its decentralized architecture, which makes it inherently secure. The distribution of the database across multiple nodes is critical to building a strong foundation for blockchain security. By implementing a cryptographic security layer that hashes block and connects them through these hashes, along with a suitable consensus mechanism, a high level of security can be achieved. Any type of data, whether it is a transaction or any other form of data, is stored permanently in a database that features these layers of security [108].

#### 7.1.5. Energy independent

The high energy consumption of blockchain technology is not due to inefficient design or devices, but rather the intentional design of the consensus algorithm. The Proof-of-Work algorithm requires a significant amount of computational power to ensure the necessary level of security. This is because a malicious node attempting to breach the network would need at least 51 % of the total computational power, which is unlikely to be achieved by a limited number of attackers. However, it is important to acknowledge the significant energy consumption resulting from this algorithm [109]. This energy dependency is particular to public blockchain architecture. In contrast, private blockchains require significantly less power, as they utilize regulated consensus algorithms such as PAXOS, RAFT, and PBFT, which do not demand high energy consumption.

#### 7.1.6. Robust

The strength of private blockchain architecture lies in the interconnection of its aspects, all of which contribute to data security. Through immutability, timestamping, and the use of consensus mechanisms, data is made secure and difficult to breach. This interplay of features makes private blockchain architecture robust and reliable [110]. Private blockchain introduces the property of an access control list, a feature does not present in public blockchains. This list dictates the privileges each node has within the network, limiting unauthorized nodes from performing actions outside their allocated roles. This enhances the network's robustness and reliability.

#### 7.1.7. Fully open source

Blockchain is built as a fully open-source platform, which allows any participant in the network to access and scrutinize the source code, ensuring full transparency. Moreover, blockchain is created using open-source materials and libraries, making it easily accessible to developers for modification and improvement. A significant advantage of its open-source nature is that the network can be customized, with policies and rules set specifically to meet the needs of the application at hand. This flexibility ensures that no restrictions hinder its implementation.

### 7.2. Weaknesses

#### 7.2.1. Interoperability

[111] discusses the current state of blockchain interoperability and highlights the growing research trends in this area, identifying it as a crucial feature of blockchain technology [112] discusses the interoperability challenges of blockchain, highlighting the difficulties in achieving seamless interoperability between different blockchain platforms without relying on a trusted third party. This issue hinders the widespread adoption of blockchain, as interoperability is crucial for collaborations between various entities, which is especially common in manufacturing and supply chain management, where multiple entities are involved in the overall system.

#### 7.2.2. Scalability

The emergence of Bitcoin brought to light the scalability challenges facing blockchain technology. Public blockchains face limitations in throughput, which is influenced by the time taken to approve a block and the size of the block. Improving one of these aspects often comes at the expense of the other, thereby making scalability a difficult problem to address [113]. Public blockchains suffer from scalability issues, particularly with transaction speed. While private blockchains are also affected by scalability problems, the impact is not as severe as in public blockchains. The scalability challenge for private blockchains lies in the complexity of implementation; as the number of nodes in a private blockchain increases, maintaining the network becomes increasingly complex.

#### 7.2.3. Storage

In a blockchain network, data is shared across a peer-to-peer network, and each node in the network has a copy of the distributed ledger, resulting in N replicas of the ledger, with N being the number of nodes in the network. As the network expands, the challenge of data storage becomes increasingly significant due to the exponential growth of storage requirements. Additionally, since the ledger is immutable, all data recorded since the creation of the network is preserved without the possibility of deletion of unused data. This issue is typically addressed by identifying and recording only the most useful data in the blockchain. However, even with such methods implemented, storage cannot be fully controlled and will face limitations as the network expands.

#### 7.2.4. Prone to sybil attacks

A potential vulnerability of blockchain is its susceptibility to sybil attacks. A Sybil attack occurs when an attacker gains control over a significant portion of the network's total computational power or nodes—often, more than 50 %, as seen in algorithms like PAXOS. When an attacker controls such a percentage, the consensus algorithm can be compromised, undermining the network's security and integrity. Although such attacks are difficult to execute, especially when the number of nodes in the network is large, they cannot be ruled out completely. Sybil attacks can trigger other types of attacks such as DoS, DDoS, majority attack, and mining pool attack as discussed by [114].

#### 7.2.5. Access challenges

Private blockchains have a unique characteristic where nodes require permission to access the network, and any action these nodes need to perform necessitates special authorization from the network provider. Although this feature works in favor of creating a more reliable and secure system, it creates a challenge to access the network freely, and results in the source code being obscured, where nodes cannot access and verify its authenticity [115]. Creating a balanced access control list that simultaneously provides the required security while allowing nodes to access their respective needed data is crucial and remains a challenging task to optimize.

#### 7.2.6. Underdeveloped technology

Various techniques utilized in blockchains such as creditworthiness, performance, efficiency, security, privacy, supervision, and online-to-offline integration are still underdeveloped [116]. This technology is relatively new, with its first implementation as Bitcoin in 2009 as a public blockchain. In late 2015, Hyperledger was founded as a private blockchain platform. Consequently, many problems and issues continue to arise and need to be addressed to achieve the widespread adoption of this technology.

#### 7.2.7. Unstandardized

When considering blockchain standards, it is crucial to note that the technology is relatively new, and early applications of the technology were not subject to any standards. However, there is now one international standardization for blockchain and distributed ledger technologies, which is ISO 22739:2020 [117].

### 7.3. Opportunities

#### 7.3.1. Eliminates third party dependency

In blockchain systems, the decentralized, peer-to-peer network architecture eliminates the need for a third-party intermediary to authenticate and validate data. This reduces the risk of malicious behavior and enhances security by allowing issues to be resolved within the network without the intervention of a third-party [118]. Instead of requiring a centralized third party to approve and store data, the ledger is distributed among all the nodes, avoiding a single point of failure (SPOF) node as described before.

#### 7.3.2. Reliable transactions

All database transactions in private blockchain are cryptographically secured through hashing, which includes the hash of the previous block, providing the first layer of security. Additionally, consensus algorithms provide an additional layer of security. As the ledger is distributed, altering any information in the database becomes exceedingly difficult. "The high level of investment by Governments and Enterprises in implementing blockchain technology for various initiatives is an indicator of potential benefits. Various pilot projects based on are ongoing, and it is being used and proposed in every domain where a secure and reliable transaction is required" [119].

#### 7.3.3. Reduce transaction costs

A substantial portion of transaction costs are attributed to the validating third party, often a bank or financial institution. Blockchain technology reduces these costs by eliminating the need for such intermediaries, enabling trusted peer-to-peer transactions directly [120].

#### 7.3.4. Increase traceability

Private blockchain provides traceability solutions in many domains [107]. A soybean traceability in the agriculture supply chain was developed on the blockchain [121]. A traceability in agri-food supply chain management was developed which is based on blockchain [122]. A decentralized traceability application for multi-tier supply chain networks in the automotive industry was developed based on blockchain [123]. All these applications demonstrate the advantages of private blockchain in manufacturing industries. The common factor among the mentioned use cases is their emphasis on high-quality standards, which are ultimately achieved through transparent traceability of data for defective products.

#### 7.3.5. Safe repository for data

The private architecture and algorithms of blockchain ensure a secure data repository that can be accessed by all members of the network. The entire database can be accessed by anyone in the network [124].

#### 7.3.6. Quality assurance

One of the major research areas for optimizing private blockchain technology is quality control. To achieve high-quality products, transparency in identifying the sources of materials, managing identities of collaborating companies, collecting relevant data, tracking shipments, and adopting similar standards are essential [87]. This, in turn, leads to high-quality and reliable products. All the above-mentioned tasks that are required to ultimately achieve high-quality production can be achieved through the implementation of private blockchain.

#### 7.3.7. Improper customer experience

Blockchain technology has a positive impact on the relationship between customers and brands by promoting transparency, trust, and security. These qualities have led to increased customer loyalty [125]. In a blockchain network, the customers can be part of the network and have a copy of the manufacturing data ledger. They can trace back the data history of the products they consume. This feature enables the customers to have comprehensive knowledge about the product, and in the case of any defect, the customer has a reliable reference for potential solutions.

### 7.4. Threats

#### 7.4.1. Privacy of confidential data

Confidentiality is paramount in medical use cases where sensitive data, including communication between the patient and clinician, should only be accessible by the patient [126]. Storing confidential data in a blockchain can pose a security risk as the data is immutable and cannot be deleted. If someone gains unauthorized access to this sensitive information, it can result in a breach of privacy and compromise the medical records of patients. Therefore, caution must be exercised when considering the use of blockchain for recording confidential medical data for example.

#### 7.4.2. Lack of technical skills

To adopt blockchain technology, specialized knowledge and skills are necessary. However, the lack of such expertise can hinder its adoption [127]. Some of the reasons for this gap in technical skills include limited availability of education and training, the complex nature of technology, its rapidly evolving pace, and the lack of industry standards. This issue becomes more critical when, after implementing blockchain networks into industrial systems, problems arise and there is a lack of technical expertise to address them. Such scenarios amplify concerns for industries considering blockchain adoption, as these issues could disrupt manufacturing processes or cause problems in supply chain operations.

#### 7.4.3. Social acceptance

Blockchain technology is widely recognized as a leading-edge technology in the modern era. Its impact on economies, businesses, and societies is significant, but the hype surrounding it can lead users to believe that it is fully developed and flawless. There is still much research needed to advance the technology to a more mature stage [128]. This poses a threat to blockchain technology adoption, as increased scrutiny and skepticism about its benefits may emerge, potentially leading to reduced societal acceptance and a negative impact on its widespread use.

#### 7.4.4. Regulation issues

The decentralized nature of private blockchain systems undermines the dominance of centralized entities such as centralized banks in the economy, leading to regulatory issues due to government skepticism towards blockchain technologies [129]. Additionally, the lack of clarity, privacy concerns, and tokenization (i.e., the conversion of real-world assets into digital ones) contribute to these regulatory challenges.

#### 7.4.5. Malicious nodes

The internet is vulnerable to various malicious activities such as identity theft, fraud, hacking, viruses, and malware, which are often initiated by malicious nodes within the network. These types of attacks are also relevant to blockchain systems [130]. Sybil attacks occur when a node creates multiple identities within a blockchain system to take over the network and initiate malicious behavior. "51 % attacks" compromises the decision-making algorithm in a network to perform detrimental activities. Eclipse attacks isolate a node from the network to manipulate its transactions. Denial of service attacks occur when a node overloads the network with traffic, hindering the ability of other nodes to communicate. While the robust security measures implemented in blockchain systems make successful cyber-attacks relatively rare, the possibility of such attacks cannot be entirely eliminated. A particularly concerning threat is the presence of a malicious node within a private blockchain that is authorized and listed on the access list. Such a node can undertake harmful actions within the network, potentially compromising its integrity.

### 7.4.6. Weak private keys

Public Key Infrastructure (PKI) is used to encrypt private blockchain data, utilizing both public and private keys. Public keys are accessible to everyone, while private keys are confidential and function as passwords [131]. Consequently, private keys are regarded as a crucial element of blockchain, as they are responsible for validating and approving transactions. Weak private keys, which are easily predictable and vulnerable, pose a threat to both the user and the blockchain system. Some of the reasons for weak private keys include improper key generation, insufficient entropy, or randomness of a key, reusing keys from other accounts, lack of awareness, and sharing private keys with untrusted parties.

### 7.4.7. Cost of maintenance

The cost of operating and maintaining a private blockchain network can escalate significantly as the network expands. When applied on a large scale, such as in a supply chain, maintaining the network can become costly due to two primary factors: the complexity of the system and the shortage of experts in the field, which limits the ability to negotiate labor costs effectively.(Table 3).

## 8. Conclusion and future work

The primary contribution of this literature review is to offer a comprehensive and centralized comparison of prominent blockchain technology architectures. This comparative analysis stems from the imperative need to identify the most suitable architecture to address the manufacturing industry's existing gaps, as identified in this review. The findings indicate that public or permissionless blockchain is acknowledged for its high level of security, attributed to its extensive used base and the implementation of robust consensus mechanism. However, its efficiency is undermined by the significant computational power needed for mining, along with the low throughput of this architecture, making it unsuitable for manufacturing applications that require fast and near real-time data exchange.

Within this context, permissioned blockchain emerges as a promising solution to bridge the identified gaps in the industry's cyber-infrastructure. This is primarily due to its capacity for rapid data processing and its appropriateness for real-time data monitoring. Additionally, private blockchains do not demand high energy overheads, as the consensus algorithms used in these architectures eliminate the need for mining, which is the primary source of high energy consumption in blockchain systems.

Both hybrid and consortium blockchains are categorized fundamentally as permissioned blockchains, sharing the common trait of combining elements from both public and private blockchain models. However, they diverge concerning the network's taxonomy: the hybrid blockchain assumes a centralized structure owned by a single authority, while the consortium blockchain operates in a decentralized manner, with all participating entities contributing to the network, thereby mitigating the risk of a single entity assuming control and jeopardizing its integrity.

Consequently, the private blockchain architecture emerges as particularly well-suited for the utilization of use cases and applications within the manufacturing industry.

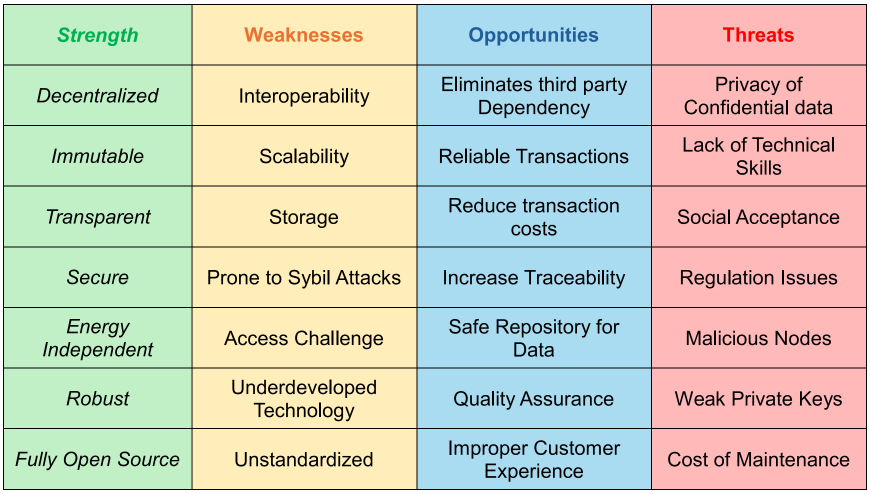
Although Hybrid and Consortium blockchains are also suitable for industrial use cases, they are slightly less favored compared to private blockchains. This is primarily due to their higher energy consumption and greater complexity in implementation. Hybrid and Consortium blockchains combine features from both private and public architectures, which not only makes them more challenging to implement but also requires more expertise to maintain effectively. In contrast, private blockchains, being more streamlined and less resource-intensive, offer a more practical solution for industrial applications as represented in Table 2.

The consensus algorithms explored in this review encompass a wide spectrum of security measures, each with its distinct advantages and disadvantages, tailored for specific applications. Nevertheless, the progression of blockchain technology depends significantly on achieving interoperability across different blockchain architectures. To attain this interoperability, a universal consensus algorithm is needed, one capable of accommodating all blockchain types, whether they are public or private.

As mentioned in section four, the existing gaps within manufacturing industries can find viable solutions through the implementation of a resilient and well-suited blockchain system. The adoption of such a system holds the potential to avoid numerous financial losses within this sector. Additionally, blockchain serves as a complementary component to cybersecurity, mutually reinforcing one another to create a highly secure environment where data infrastructure can be both dependable and fortified.

Section five begins with a holistic comparison of the four discussed blockchain architectures, quantifying their features with scores to

**Table 3**
SWOT Analysis Summary.



| *Strength* | Weaknesses | Opportunities | Threats |
|---|---|---|---|
| *Decentralized* | Interoperability | Eliminates third party Dependency | Privacy of Confidential data |
| *Immutable* | Scalability | Reliable Transactions | Lack of Technical Skills |
| *Transparent* | Storage | Reduce transaction costs | Social Acceptance |
| *Secure* | Prone to Sybil Attacks | Increase Traceability | Regulation Issues |
| *Energy Independent* | Access Challenge | Safe Repository for Data | Malicious Nodes |
| *Robust* | Underdeveloped Technology | Quality Assurance | Weak Private Keys |
| *Fully Open Source* | Unstandardized | Improper Customer Experience | Cost of Maintenance |

establish a common ground for comparison. This approach allows for a clear evaluation of each architecture's strengths and weaknesses in relation to manufacturing use cases. Based on this comprehensive assessment, the private blockchain architecture was identified as the most suitable option. Following this analysis, the section continues by conducting a comprehensive SWOT analysis which focused on private blockchain, providing an in-depth examination of its strengths, weaknesses, opportunities, and threats. This analysis, in essence, serves as a catalyst for future research endeavors, directing attention towards areas within this architecture that have yet to receive extensive scholarly research. Notably, the weaknesses and threats sections of the analysis pinpoint specific challenges inherent to this type of blockchain. Each of these challenges can potentially serve as a distinct research domain. Addressing these challenges and mitigating associated threats has the potential to pave the way for the development of a resilient and robust blockchain system.

A critical aspect that demands attention in blockchain research is the regulatory challenges associated with this technology. As highlighted in the SWOT analysis, the privacy of confidential data presents a significant threat. Once data is recorded in a blockchain database, it cannot be removed, posing a substantial risk if accessed by unauthorized parties. This threat is largely due to the current lack of regulation governing what data should or should not be stored on the blockchain. However, blockchain operates on a decentralized framework, while regulation typically requires centralized authority, creating a fundamental contradiction. Therefore, it is essential to find a balance or develop an approach to establish regulation within a decentralized system.

Blockchain technology is relatively new, offering vast opportunities for exploration across various domains. However, its widespread adoption in the manufacturing industry is hindered by significant challenges, particularly in scalability and interoperability. Targeted research efforts to address these and other existing issues could serve as a catalyst for broader implementation and optimization of blockchain technology. Additionally, the weaknesses and threats identified in the SWOT analysis highlight potential research areas that merit further investigation.

Federated learning is a key innovation in manufacturing that enhances collaboration between facilities. Rather than sharing raw data, each facility trains machine learning models on its own data and then shares model parameters to update those used by other facilities. In essence, federated learning operates as a decentralized system, and its synergy with blockchain technology is particularly powerful. Blockchain can be leveraged to create a secure environment for sharing these updated parameters, ensuring that each facility's contributions are both secure and verifiable, thereby fostering a trustworthy and collaborative manufacturing ecosystem. Further investigation into this domain is essential.

Finally, a summary of the prominent hurdles facing blockchain technology is presented below to guide future research:

- **Scalability:** Current blockchain frameworks have limited capacity and face challenges as the network grows. This is particularly critical in industrial applications, such as supply chain management, where a high number of nodes may join the network, and large volumes of data must be efficiently processed.
- **Interoperability:** Numerous blockchain platforms exist, each with their own architecture—whether public, private, or otherwise—and specific consensus algorithms tailored to their applications. However, these platforms often operate in isolation, unable to communicate with one another, which limits collaboration and connectivity between different entities. Focusing research on enabling seamless communication between different blockchains, without relying on third-party software, is essential for enhancing interoperability.
- **Storage:** A fundamental characteristic of blockchain databases is their immutability, meaning that data recorded within the database cannot be altered or deleted, and remains permanently stored. Additionally, because blockchain is decentralized, every node in the network holds a copy of the entire database. As the network grows, the size of the database will continue to expand, leading to significant storage concerns. Finding solutions to address these storage challenges is crucial as blockchain networks scale over time.
- **Lack of Standardization:** As a relatively new technology, blockchain lacks standardized protocols, with each platform adhering to its own specific standards and practices. This lack of standardization hinders the integration of different blockchains and impedes interoperability, as seamless communication between blockchain platforms requires a common foundational framework. Standardizing this technology is imperative and should be a key focus of ongoing research.
- **Regulation Issues:** Blockchain technology is currently not regulated, which presents a challenge due to its decentralized nature. Regulating the technology could conflict with its fundamental principle of decentralization. However, finding a balance that maintains decentralization while incorporating beneficial regulations could optimize the system. Such regulations would not only enhance the technology but also increase social acceptance, as people tend to trust systems with established regulatory frameworks. Addressing this issue should be a focus of ongoing research to support the widespread adoption of blockchain technology.

The listed hurdles represent some of the most prominent challenges that blockchain technology is currently facing. For a more comprehensive overview and a broader list of issues, refer to the SWOT analysis in Section 5, which details the weaknesses and threats associated with blockchain. Each of these aspects presents potential areas for further research.

## CRediT authorship contribution statement

**Ramy Harik:** Conceptualization, Funding acquisition, Methodology, Supervision, Writing – review & editing. **Philip Samaha:** Conceptualization, Formal analysis, Methodology, Writing – original draft. **Fadi El Kalach:** Conceptualization, Methodology, Writing – review & editing.

## Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the author(s) used "ChatGPT" to improve the readability, grammar correction, and language of the paper. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

This work is funded in part by NSF Award 2119654 "RII Track 2 FEC: Enabling Factory to Factory (F2F) Networking for Future Manufacturing," and "Enabling Factory to Factory (F2F) Networking for Future Manufacturing across South Carolina," funded by South Carolina Research Authority. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsors.

## References

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

[2] A.H. Lone and R. Naaz, Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review, 2021. doi: 10.1016/j.cosrev.2020.100360.

[3] T.K. Dasaklis, T.G. Voutsinas, G.T. Tsoulfas, F. Casino, A Systematic Literature Review of Blockchain-Enabled Supply Chain Traceability Implementations," 2022. doi: 10.3390/su14042439.

[4] H. Huang, W. Kong, S. Zhou, Z. Zheng, S. Guo, A Survey of State-of-The-Art on Blockchains, 2021. doi: 10.1145/3441692.

[5] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," 2021. doi: 10.1016/j.bcra.2021.100027.

[6] M. Krichen, M. Ammi, A. Mihoub, M. Almutiq, Blockchain for Modern Applications: A Survey, 2022. doi: 10.3390/s22145274.

[7] Abdelrahman N, Farah A. Blockchain technology: classification, opportunities, and challenges. Int Res J Eng Technol (IRJET) 2018;5(5).

[8] B. Shrimali and H.B. Patel, Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities, 2021. doi: 10.1016/j.jksuci.2021.08.005.

[9] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, S. Shimizu, Privacy preservation in permissionless blockchain: A survey, 2021. doi: 10.1016/j.dcan.2020.05.008.

[10] Rankhambe BP, Kaur Khanuja H. A comparative analysis of blockchain platforms - bitcoin and ethereum,. Proc - 2019 5th Int Conf Comput, Commun Control Autom, ICCUBEA 2019 2019. https://doi.org/10.1109/ICCUBEA47591.2019.9129332.

[11] Chauhan A, Malviya OP, Verma M, Mor TS. Blockchain and scalability. Proc - 2018 IEEE 18th Int Conf Softw Qual, Reliab, Secur Companion, QRS-C 2018 2018. https://doi.org/10.1109/QRS-C.2018.00034.

[12] Solat S, Calvez P, Naït-Abdesselam F. Permissioned vs. permissionless blockchain: how and why there is only one right choice. J Softw 2021:95–106. https://doi.org/10.17706/jsw.16.3.95-106.

[13] D. Khan, L.T. Jung, M.A. Hashmani, Systematic literature review of challenges in blockchain scalability, 2021. doi: 10.3390/app11209372.

[14] Yusoff J, Mohamad Z, Anuar M. A review: consensus algorithms on blockchain. J Comput Commun 2022;10(09). https://doi.org/10.4236/jcc.2022.109003.

[15] Golosova J, Romanovs A. Overview of the blockchain technology cases. 59th Int Sci Conf Inf Technol Manag Sci Riga Tech Univ, ITMS 2018 - Proc 2018. https://doi.org/10.1109/ITMS.2018.8552978.

[16] Bischoff O, Seuring S. Opportunities and limitations of public blockchain-based supply chain traceability. Mod Supply Chain Res Appl 2021;3(3). https://doi.org/10.1108/mscra-07-2021-0014.

[17] M. Platt and P. McBurney, Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance, 2023. doi: 10.3390/a16010034.

[18] N.O. Nawari and S. Ravindran, Blockchain and the built environment: Potentials and limitations, 2019. doi: 10.1016/j.jobe.2019.100832.

[19] Gracy M, Rebecca Jeyavadhanam B. A systematic review of blockchain-based system: transaction throughput latency and challenges. 2021 Int Conf Comput Intell Comput Appl, ICCICA 2021 2021. https://doi.org/10.1109/ICCICA52458.2021.9697142.

[20] D. Cagigas, J. Clifton, D. Diaz-Fuentes, M. Fernandez-Gutierrez, Blockchain for Public Services: A Systematic Literature Review, 2021. doi: 10.1109/ACCESS.2021.3052019.

[21] I. Vinivius Alvarenga Marinelli, Blockchain technology applications for financial transparency in non profit organizations, 2019.

[22] Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V. Blockchain and smart contracts for insurance: is the technology mature enough? Future Internet 2018;10(2). https://doi.org/10.3390/fi10020020.

[23] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 2016;40(10). https://doi.org/10.1007/s10916-016-0574-6.

[24] Dong C, Wang Y, Aldweesh A, McCorry P, Van Moorsel A. Betrayal, distrust, and Rationality: Smart counter-collusion contracts for verifiable cloud computing. Proc ACM Conf Comput Commun Secur 2017. https://doi.org/10.1145/3133956.3134032.

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

[26] McCorry P, Shahandashti SF, Hao F. A smart contract for boardroom voting with maximum voter privacy. Lect Notes Comput Sci (Incl Subser Lect Notes Artif Intell Lect Notes Bioinforma 2017. https://doi.org/10.1007/978-3-319-70972-7_20.

[27] Wang G, Nixon M. SoK: Tokenization on blockchain. ACM Int Conf Proc Ser 2021. https://doi.org/10.1145/3492323.3495577.

[28] Ihle C, Trautwein D, Schubotz M, Meuschke N, Gipp B. Incentive mechanisms in peer-to-peer networks - a systematic literature review. ACM Comput Surv 2023; 55(14 s). https://doi.org/10.1145/3578581.

[29] Ismail L, Materwala H. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. Symmetry 2019;11(10). https://doi.org/10.3390/sym11101198.

[30] Polge J, Robert J, Le Traon Y. Permissioned blockchain frameworks in the industry: a comparison. ICT Express 2021;7(2). https://doi.org/10.1016/j.icte.2020.09.002.

[31] Sukhwani H, Martínez JM, Chang X, Trivedi KS, Rindos A. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). Proc IEEE Symp Reliab Distrib Syst 2017. https://doi.org/10.1109/SRDS.2017.36.

[32] Yang R, et al. Public and private blockchain in construction business process and information integration. " *Autom Constr* 2020;118. https://doi.org/10.1016/j.autcon.2020.103276.

[33] Bada AO, Damianou A, Angelopoulos CM, Katos V. Towards a green blockchain: a review of consensus mechanisms and their energy consumption. Proc - 17th Annu Int Conf Distrib Comput Sens Syst, DCOS 2021 2021. https://doi.org/10.1109/DCOSS52077.2021.00083.

[34] Idrees SM, Nowostawski M, Jameel R, Mourya AK. Security aspects of blockchain technology intended for industrial applications. Electronics 2021;10(8). https://doi.org/10.3390/electronics10080951.

[35] Ncube T, Dlodlo N, Terzoli A. Private blockchain networks: a solution for data privacy. 2020 2nd Int Multidiscip Inf Technol Eng Conf, IMITEC 2020 2020. https://doi.org/10.1109/IMITEC50163.2020.9334132.

[36] Okeme PA, Skakun AD, Muzalevskii AR. Transformation of factory to smart factory. Proc 2021 IEEE Conf Russ Young– Res Electr Electron Eng ElConRus 2021 2021. https://doi.org/10.1109/ElConRus51938.2021.9396278.

[37] Shamshad S, Minahil, Mahmood K, Kumari S, Chen CM. A secure blockchain-based e-health records storage and sharing scheme. J Inf Secur Appl 2020;55. https://doi.org/10.1016/j.jisa.2020.102590.

[38] A. Alkhateeb, C. Catal, G. Kar, A. Mishra, Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review, 2022. doi: 10.3390/s22041304.

[39] Hu J, Reed MJ, Al-Naday M, Thomos N. Hybrid blockchain for IoT—energy analysis and reward plan. Sens (Switz) 2021;21(1). https://doi.org/10.3390/s21010305.

[40] Sagirlar G, Carminati B, Ferrari E, Sheehan JD, Ragnoli E. Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-Blockchains. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE; Jul. 2018. p. 1007–16. https://doi.org/10.1109/Cybermatics_2018.2018.00189.

[41] Dib O, Brousmiche K, Durand A, Thea E, Hamida B. Consortium blockchains: overview, applications and challenges. Int J Adv Telecommun 2018;11(1 & 2).

[42] Nijsse J, Litchfield A. A taxonomy of blockchain consensus methods. Cryptography 2020;4(4). https://doi.org/10.3390/cryptography4040032.

[43] Rebello GAF, Camilo GF, Guimarães LCB, de Souza LAC, Thomaz GA, Duarte OCMB. A security and performance analysis of proof-based consensus protocols. Ann Des Telecommun/Ann Telecommun 2022;77(7–8). https://doi.org/10.1007/s12243-021-00896-2.

[44] C. Schinckus, Proof-of-work based blockchain technology and Anthropocene: An undermined situation?, 2021. doi: 10.1016/j.rser.2021.111682.

[45] Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Čapkun S. On the security and performance of Proof of Work blockchains. Proc ACM Conf Comput Commun Secur 2016. https://doi.org/10.1145/2976749.2978341.

[46] Li SN, Yang Z, Tessone CJ. Proof-of-Work cryptocurrency mining: a statistical approach to fairness. 2020 IEEE/CIC Int Conf Commun China, ICCC Workshops 2020 2020. https://doi.org/10.1109/ICCCWorkshops49972.2020.9209934.

[47] Zhang X, Qin R, Yuan Y, Wang FY. An analysis of blockchain-based bitcoin mining difficulty: techniques and principles. Proc 2018 Chin Autom Congr, CAC 2018 2018. https://doi.org/10.1109/CAC.2018.8623140.

[48] S.M.H. Bamakan, A. Motavali, A. Babaei Bondarti, A survey of blockchain consensus algorithms performance evaluation criteria, 2020. doi: 10.1016/j.eswa.2020.113385.

[49] Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access 2019;7. https://doi.org/10.1109/ACCESS.2019.2925010.

[50] Shifferaw Y, Lemma S. "Limitations of proof of stake algorithm in blockchain: a review. Zede J 2021;39(1).

[51] Koštál K, Krupa T, Gembec M, Vereš I, Ries M, Kotuliak I. On transition between PoW and PoS. Proc Elmar - Int Symp Electron Mar 2018. https://doi.org/10.23919/ELMAR.2018.8534642.

[52] Kaur M, Khan MZ, Gupta S, Noorwali A, Chakraborty C, Pani SK. MBCP: performance analysis of large scale mainstream blockchain consensus protocols. IEEE Access 2021;9. https://doi.org/10.1109/ACCESS.2021.3085187.

[53] Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of activity: extending bitcoin's proof of work via proof of stake. Cryptol EPrint Arch 2014;452(3).

[54] Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of activity: extending bitcoin's proof of work via proof of stake [extended abstract]. ACM SIGMETRICS Perform Eval Rev 2014;42(3).

[55] Xiao B, Jin C, Li Z, Zhu B, Li X, Wang D. Proof of Importance: A Consensus Algorithm for Importance Based on Dynamic Authorization. ACM International Conference Proceeding Series; 2021. https://doi.org/10.1145/3498851.3499007.

[56] Aslam T, et al. Blockchain based enhanced ERP transaction integrity architecture and PoET consensus. Comput, Mater Contin 2021;70(1). https://doi.org/10.32604/cmc.2022.019416.

[57] L. Lamport, "Paxos Made Simple," ACM SIGACT News, vol. 32, no. 4, 2001.

[58] Xiao Y, Zhang N, Lou W, Hou YT. A survey of distributed consensus protocols for blockchain networks. IEEE Commun Surv Tutor 2020;22(2). https://doi.org/10.1109/COMST.2020.2969706.

[59] Hu J, Liu K. Raft consensus mechanism and the applications. J Phys Conf Ser 2020. https://doi.org/10.1088/1742-6596/1544/1/012079.

[60] H and H.M. Kull, Secure log-management for an Apache Kafka-based data-streaming service, 2023.

[61] J. Kreps, N. Narkhede, J. Rao, Kafka: a Distributed Messaging System for Log Processing, ACM SIGMOD Workshop on Networking Meets Databases, 2011.

[62] Wang R, Zhang L, Xu Q, Zhou H. K-Bucket based raft-like consensus algorithm for permissioned blockchain. Proc Int Conf Parallel Distrib Syst - ICPADS 2019. https://doi.org/10.1109/ICPADS47876.2019.00152.

[63] X. Fu, H. Wang, P. Shi, A survey of Blockchain consensus algorithms: mechanism, design and applications, 2021. doi: 10.1007/s11432–019-2790–1.

[64] Bazzi RA, Neiger G. Simplifying fault-tolerance: providing the abstraction of crash failures. J ACM 2001;48(3). https://doi.org/10.1145/382780.382784.

[65] Lamport L, Shostak R, Pease M. The byzantine generals problem. ACM Trans Program Lang Syst (TOPLAS) 1982;4(3). https://doi.org/10.1145/357172.357176.

[66] Castro M, Liskov B. Practical byzantine fault tolerance. Proc Symp Oper Syst Des Implement 1999;(February). https://doi.org/10.1145/571637.571640.

[67] Yao W, Ye J, Murimi R, Wang G. A survey on consortium blockchain consensus mechanisms. Int J Adv Telecom 2018;11(1).

[68] Li W, Feng C, Zhang L, Xu H, Cao B, Imran MA. A scalable multi-layer PBFT consensus for blockchain. IEEE Trans Parallel Distrib Syst 2021;32(5). https://doi.org/10.1109/TPDS.2020.3042392.

[69] Zhang J, Rong Y, Cao J, Rong C, Bian J, Wu W. DBFT: a byzantine fault tolerance protocol with graceful performance degradation. IEEE Trans Dependable Secur Comput 2022;19(5). https://doi.org/10.1109/TDSC.2021.3095544.

[70] Singh A, Click K, Parizi RM, Zhang Q, Dehghantanha A, Choo K-KR. Sidechain technologies in blockchain networks: an examination and state-of-the-art review. J Netw Comput Appl Jan. 2020;149:102471. https://doi.org/10.1016/j.jnca.2019.102471.

[71] Sanka AI, Cheung RCC. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. J Netw Comput Appl Dec. 2021;195:103232. https://doi.org/10.1016/j.jnca.2021.103232.

[72] Kim S, Kwon Y, Cho S. A Survey of Scalability Solutions on Blockchain. 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE; Oct. 2018. p. 1204–7. https://doi.org/10.1109/ICTC.2018.8539529.

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

[74] T. Hewa, M. Ylianttila, M. Liyanage, Survey on blockchain based smart contracts: Applications, opportunities and challenges, 2021. doi: 10.1016/j.jnca.2020.102857.

[75] Prashanth Joshi A, Han M, Wang Y. A survey on security and privacy issues of blockchain technology. Math Found Comput 2018;1(2):121–47. https://doi.org/10.3934/mfc.2018007.

[76] S.E. Chang and Y. Chen, When blockchain meets supply chain: A systematic literature review on current development and potential applications, 2020. doi: 10.1109/ACCESS.2020.2983601.

[77] Nasir MH, Arshad J, Khan MM, Fatima M, Salah K, Jayaraman R. Scalable blockchains — a systematic review. Future Gener Comput Syst 2022;126. https://doi.org/10.1016/j.future.2021.07.035.

[78] J. Fernando, Supply Chain Management (SCM): How It Works and Why It Is Important, Investopedia, 2023.

[79] Viriyasitavat W, Bi Z, Hoonsopon D. Blockchain technologies for interoperation of business processes in smart supply chains. J Ind Inf Integr 2022;26. https://doi.org/10.1016/j.jii.2022.100326.

[80] Wu Y, Zhang Y. An integrated framework for blockchain-enabled supply chain trust management towards smart manufacturing. Adv Eng Inform 2022;51. https://doi.org/10.1016/j.aei.2021.101522.

[81] A. Raja Santhi and P. Muthuswamy, "Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics," 2022. doi: 10.3390/logistics6010015.

[82] Jabbar S, Lloyd H, Hammoudeh M, Adebisi B, Raza U. Blockchain-enabled supply chain: analysis, challenges, and future directions. Multimed Syst 2021. https://doi.org/10.1007/s00530-020-00687-0.

[83] Schmidt CG, Wagner SM. Blockchain and supply chain relations: a transaction cost theory perspective. J Purch Supply Manag 2019;25(4). https://doi.org/10.1016/j.pursup.2019.100552.

[84] Singh M, Kim S. Branch based blockchain technology in intelligent vehicle. Comput Netw 2018;145. https://doi.org/10.1016/j.comnet.2018.08.016.

[85] Silas Nzuva. Smart contracts implementation, applications, benefits, and limitations. J Inf Eng Appl 2019. https://doi.org/10.7176/JIEA/9-5-07.

[86] Chen S, Shi R, Ren Z, Yan J, Shi Y, Zhang J. A Blockchain-Based Supply Chain Quality Management Framework. 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE). IEEE; 2017. p. 172–6. https://doi.org/10.1109/ICEBE.2017.34.

[87] Shahbazi Z, Byun YC. Integration of blockchain, iot and machine learning for multistage quality control and enhancing security in smart manufacturing. Sensors 2021;21(4). https://doi.org/10.3390/s21041467.

[88] Chen S, et al. Blockchain applications in PLM towards smart manufacturing. Int J Adv Manuf Technol 2022;118(7–8). https://doi.org/10.1007/s00170-021-07802-z.

[89] Jhala KS, Oak R, Khare M. Smart collaboration mechanism using blockchain technology. in Proceedings - 5th IEEE International Conference on Cyber Security and Cloud Computing and 4th IEEE International Conference on Edge Computing and Scalable Cloud, CSCloud/EdgeCom 2018. 2018. https://doi.org/10.1109/CSCloud/EdgeCom.2018.00029.

[90] Savelyev A. Copyright in the blockchain era: promises and challenges. Comput Law Secur Rev 2018;34(3). https://doi.org/10.1016/j.clsr.2017.11.008.

[91] Yousif I, Burns L, El Kalach F, Harik R. Leveraging computer vision towards high-efficiency autonomous industrial facilities. J Intell Manuf 2024. https://doi.org/10.1007/s10845-024-02396-1.

[92] Zugarramurdi A, Parin MA, Gadaleta L, Carrizo G, Lupin HM. The effect of improving raw material quality on product quality and operating costs: a comparative study for lean and fatty fish. Food Control 2004;15(7). https://doi.org/10.1016/j.foodcont.2003.08.001.

[93] Li X. Inventory management and information sharing based on blockchain technology. Comput Ind Eng 2023;179. https://doi.org/10.1016/j.cie.2023.109196.

[94] Zhang Y, Xu X, Liu A, Lu Q, Xu L, Tao F. Blockchain-based trust mechanism for iot-based smart manufacturing system. IEEE Trans Comput Soc Syst 2019;6(6). https://doi.org/10.1109/TCSS.2019.2918467.

[95] Yu K, Tan L, Aloqaily M, Yang H, Jararweh Y. Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. IEEE Trans Ind Inf 2021;17(11). https://doi.org/10.1109/TII.2021.3049141.

[96] Dhar S, Bose I. Securing IoT devices using zero trust and blockchain. J Organ Comput Electron Commer 2021;31(1). https://doi.org/10.1080/10919392.2020.1831870.

[97] Iqbal A, Amir M, Kumar V, Alam A, Umair M. Integration of next generation IIoT with blockchain for the development of smart industries (no. Special Issue) Emerg Sci J 2020;4. https://doi.org/10.28991/esj-2020-SP1-01.

[98] Q. Wang, X. Zhu, Y. Ni, L. Gu, H. Zhu, Blockchain for the IoT and industrial IoT: A review, 2020. doi: 10.1016/j.iot.2019.100081.

[99] F. Elghaish et al., Blockchain and the 'Internet of Things'' for the construction industry: research trends and opportunities, 2021. doi: 10.1016/j.autcon.2021.103942.

[100] Tian Y, Li T, Xiong J, Bhuiyan MZA, Ma J, Peng C. A blockchain-based machine learning framework for edge services in IIoT. IEEE Trans Ind Inf 2022;18(3). https://doi.org/10.1109/TII.2021.3097131.

[101] Kaynak B, Kaynak S, Uygun Ö. Cloud manufacturing architecture based on public blockchain technology. IEEE Access 2020;8. https://doi.org/10.1109/ACCESS.2019.2962232.

[102] Vatankhah Barenji R. A blockchain technology based trust system for cloud manufacturing. J Intell Manuf 2022;33(5). https://doi.org/10.1007/s10845-020-01735-2.

[103] Egress, Five biggest supply chain compromise attacks of 2022, 〈https://www.egress.com/blog/phishing/biggest-supply-chain-compromise-attacks〉.

[104] Ponemon Institute and IBM Security, "Cost of a data breach 2022," IBM Corportation and Ponemon Institute Research, 2022.

[105] Puthal D, Malik N, Mohanty SP, Kougianos E, Yang C. The blockchain as a decentralized security framework future directions. IEEE Consum Electron Mag 2018;7(2). https://doi.org/10.1109/MCE.2017.2776459.

[106] Rajasekaran AS, Azees M, Al-Turjman F. A comprehensive survey on blockchain technology. Sustain Energy Technol Assess 2022;52. https://doi.org/10.1016/j.seta.2022.102039.

[107] Sunny J, Undralla N, Madhusudanan Pillai V. Supply chain transparency through blockchain-based traceability: an overview with demonstration. Comput Ind Eng 2020;150. https://doi.org/10.1016/j.cie.2020.106895.

[108] Stephen R, Alex A. A review on BlockChain security. IOP Conf Ser: Mater Sci Eng 2018. https://doi.org/10.1088/1757-899X/396/1/012030.

[109] Sedlmeir J, Buhl HU, Fridgen G, Keller R. The energy consumption of blockchain technology: beyond myth. Bus Inf Syst Eng 2020;62(6). https://doi.org/10.1007/s12599-020-00656-x.

[110] Bodkhe U, et al. Blockchain for Industry 4.0: a comprehensive review. IEEE Access 2020;8. https://doi.org/10.1109/ACCESS.2020.2988579.

[111] Belchior R, Vasconcelos A, Guerreiro S, Correia M. A survey on blockchain interoperability: past, present, and future trends. ACM Comput Surv 2022;54(8):1–41. https://doi.org/10.1145/3471140.

[112] Lafourcade P, Lombard-Platet M. About blockchain interoperability. Inf Process Lett 2020;161:105976. https://doi.org/10.1016/j.ipl.2020.105976.

[113] Zhou Q, Huang H, Zheng Z, Bian J. Solutions to scalability of blockchain: a survey. IEEE Access 2020;8. https://doi.org/10.1109/aCCESS.2020.2967218.

[114] Swathi P, Modi C, Patel D. Preventing Sybil Attack in Blockchain using Distributed Behavior Monitoring of Miners. 2019 10th Int Conf Comput, Commun Netw Technol, ICCCNT 2019 2019. https://doi.org/10.1109/ICCCNT45670.2019.8944507.

[115] Bedin ARC, Capretz M, Mir S. Blockchain for collaborative businesses. Mob Netw Appl 2021;26(1). https://doi.org/10.1007/s11036-020-01649-6.

[116] Y. Li, Emerging blockchain-based applications and techniques, 2019. doi: 10.1007/s11761–019-00281-x.

[117] ANSI, "Blockchain and Cryptocurrency Standards," 〈https://blog.ansi.org/blockchain-cryptocurrency-standards-iso-ieee/#gref〉.

[118] Xu S, Chen X, He Y. EVchain: an anonymous blockchain-based system for charging-connected electric vehicles. Tsinghua Sci Technol 2021;26(6). https://doi.org/10.26599/TST.2020.9010043.

[119] Alam S, et al. Blockchain-based Initiatives: current state and challenges. Comput Netw 2021;198. https://doi.org/10.1016/j.comnet.2021.108395.

[120] Khan AG, Zahid AH, Hussain M, Farooq M, Riaz U, Alam TM. A journey of WEB and blockchain towards the industry 4.0: an overview. 3rd Int Conf Innov Comput, ICIC 2019 2019. https://doi.org/10.1109/ICIC48496.2019.8966700.

[121] Salah K, Nizamuddin N, Jayaraman R, Omar M. Blockchain-based soybean traceability in agricultural supply chain. IEEE Access 2019;7. https://doi.org/10.1109/ACCESS.2019.2918000.

[122] Caro MP, Ali MS, Vecchio M, Giaffreda R. Blockchain-based traceability in Agri-Food supply chain management: a practical implementation. 2018 IOT Vert Top Summit Agric - Tuscany, IOT Tuscany 2018 2018. https://doi.org/10.1109/IOT-TUSCANY.2018.8373021.

[123] Miehle D, Henze D, Seitz A, Luckow A, Bruegge B. PartChain: A decentralized traceability application for multi-tier supply chain networks in the automotive industry. Proc - 2019 IEEE Int Conf Decentralized Appl Infrastruct, DAPPCON 2019 2019. https://doi.org/10.1109/DAPPCON.2019.00027.

[124] Q. Mamun, Blockchain technology in the future of healthcare, 2022. doi: 10.1016/j.smhl.2021.100223.

[125] iCommunity Labs,Improved customer experience with blockchain, ⟨https://icommunity.io/en/improved-customer-experience-with-blockchain⟩.

[126] Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain. AMIA Annu Symp Proc 2017;2017.

[127] Dehghani M, William Kennedy R, Mashatan A, Rese A, Karavidas D. High interest, low adoption. A mixed-method investigation into the factors influencing organisational adoption of blockchain technology. J Bus Res 2022;149. https://doi.org/10.1016/j.jbusres.2022.05.015.

[128] Dhaliwal A, Malik S. Acceptance and adoption of blockchain technology: an examination of the security & privacy challenges. Block Bus: How it Works Creat Value 2021. https://doi.org/10.1002/9781119711063.ch11.

[129] A.A. Monrat, O. Schelén, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, 2019. doi: 10.1109/ACCESS.2019.2936094.

[130] Xu JJ. Are blockchains immune to all malicious attacks? Financ Innov 2016;2(1). https://doi.org/10.1186/s40854-016-0046-5.

[131] M.P. McBee and C. Wilcox, Blockchain Technology: Principles and Applications in Medical Imaging, 2020. doi: 10.1007/s10278–019-00310–3.