# Blockchain Protocols & Edge Computing Targeting Industry 5.0 Needs

Miguel Oliveira *, Sumit Chauhan, Filipe Alexandre Pereira, Manuel Carlos Felgueiras, David Vieira Carvalho

Posted Date: 16 June 2023

doi: 10.20944/preprints202306.1159.v1

Keywords: blockchain; protocols; Industry 5.0; sensing; 5G networks

*Article*

# Blockchain Protocols & Edge Computing Targeting Industry 5.0 Needs

**Miguel Oliveira [1,*], Sumit Chauhan [2], Filipe Pereira [3], Carlos Felgueiras [4] and David Carvalho[5]**

[1] Aveiro-North Polytechnic School, University of Aveiro; miguel@ua.pt
[2] Naoris Protocol; sumit@@naoris.com
[3] Oporto Higher Institute of Engineering, Oporto Polytechnic School, fal@isep.ipp.pt
[4] Oporto Higher Institute of Engineering, Oporto Polytechnic School; mcf@isep.ipp.pt
[5] Naoris Protocol; david@@naoris.com

**Abstract:** "Industry 5.0" is the latest industrial revolution. A variety of cutting-edge technologies, including artificial intelligence, the Internet of Things (IoT), and others, come together to form it. Billions of devices are connected for high-speed data transfer, especially in a 5G-enabled industrial environment for information collection and processing. Most of the issues such as access control mechanism, time to fetch the data from different devices, and protocols used may not be applicable in the future as these protocols are based upon a centralized mechanism. This centralized mechanism may have a single point of failure along with the computational overhead. So, there is a need for an efficient decentralized access control mechanism for device-to-device (D2D) communication in various industrial sectors, for example, sensors in different regions may collect and process the data for making intelligent decisions. In such an environment, reliability, security and privacy are major concerns as most of the solutions are based upon the centralized control mechanism. To mitigate the aforementioned issues, this paper provides the opportunities and highlights towards some most impressive initiatives that help to curve the future. This new era will bring about significant changes in the way businesses operate, allowing them to become more cost-effective, more efficient, and produce higher-quality goods and services. Because sensors are getting more accurate, cheaper, and lower time response, 5G networks are being put in place, and more industrial equipment and machinery are becoming available, various sectors including manufacturing sector is going through a significant period of transition right now. Additionally, the emerge of the cloud enables modern production models that use the cloud (both internal and external services), networks, and systems to leverage the cloud's low cost, scalability, increased computational power, real-time communication, and data transfer capabilities to create much smarter and more autonomous systems. We discuss the ways in which decentralized networks that make use of protocols help to achieve decentralization and how network meshes can grow to make things more secure, reliable and cohere with these technologies, which are not going away anytime soon. We emphasize the significance of new design in regard to cybersecurity, data integrity, and storage by using straightforward examples that have the potential to lead to the excellence of distributed systems.

- This groundbreaking paper delves deep into the world of industrial automation and explores the possibilities to adopt blockchain for developing solution for Smart City, Smart Home, Healthcare, Smart Agriculture, Autonomous Vehicles, and Supply Chain Management within Industry 5.0. With an in-depth examination of various consensus mechanisms, readers gain a comprehensive understanding of the latest developments in this field.

- The paper also explores the current issues and challenges associated with blockchain adaptation for industrial automation and provides a thorough comparison of the available consensus, enabling end customers to select the most suitable one based on its unique advantages.

- Case studies highlight how to enable adoption of blockchain in Industry 5.0 solutions effectively and efficiently, offering valuable insights into the potential challenges that lie ahead, particularly for smart industrial applications.

**Keywords:** blockchain; edge computing; protocols; Industry 5.0; sensing; 5G networks

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 June 2023 doi:10.20944/preprints202306.1159.v1



## 1. Introduction

When discussing 5G networks, sensing is becoming an increasingly important touchstone. These devices, which include sensors that measure or detect physical phenomena and transducers, produce a large amount of data that can have a significant impact on the management of production as well as the efficiency with which it operates. The growth of sensors in the Industrial Internet of Things (IIoT) is important for the growth of automated manufacturing [1]. The vast majority of the work that humans were once responsible for in each, and every industrial physical process can now be done by sensors, which are both more accurate and less expensive (Figure 1).

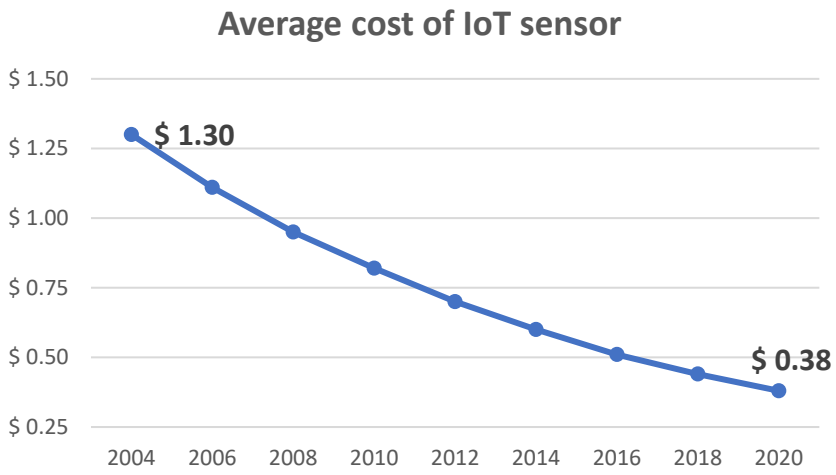
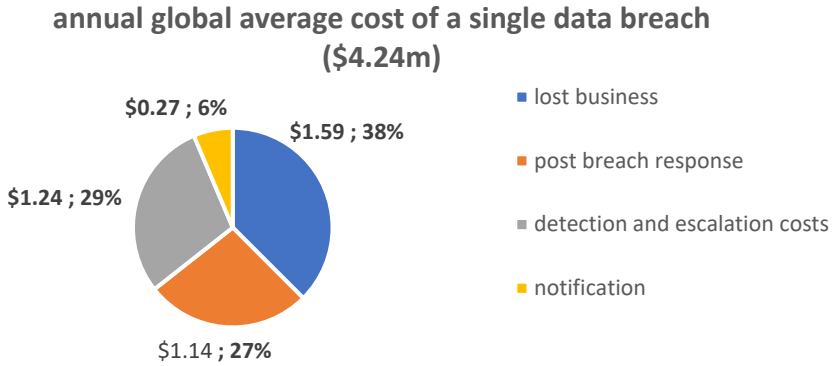



**Figure 1.** Average cost of IoT sensor [2].

In the previous chart is presented data of 2019 because it is the most accurate stats that are available since the pandemic crisis. Even though the use of sensors has increased over the past few years, they still present new challenges in terms of data and communication. These challenges include the necessity of ensuring that the data is accurate, the volume of data, the amount of time it takes to send it, and the manner in which it needs to be processed.

It is possible for a variety of issues to arise if data integrity is not maintained for a variety of reasons. Some of these issues include data breaches, the loss of access to data sets, incoherence in production databases, and many others. In a recent study by IBM [3], the annual global average cost of a data breach was estimated to be $4.24 million, while the cost of lost business was estimated to be $1.59 million, or 38% of the total cost. Lost business includes business disruption and revenue losses from system downtime, the cost of losing customers and gaining new ones, reputation losses, and decreased goodwill. Secondly, the detection and escalation costs represent $1.24 million (29%) of the total cost, followed by post-breach response, costs of $1.14 million (27%) and notification, $0.27 million (6%).



 doi:10.20944/preprints202306.1159.v1



**Figure 2.** Average cost of a data breach [3].

In the previous chart is presented data of 2019 because it is the most accurate stats that are available since the pandemic crisis. In the report [3] it is predicted that the amount of data that will be created in the year 2021 is estimated to be 79 zettabytes [4], even though "less than 0.5% of all data is ever analyzed and used" [5]. This occurs for a variety of reasons, including limited budgets for data analysis, poor data integration tools, manual data entry and collection processes, multiple standalone and distributed analytical tools, poor auditing procedures, and a lack of reliance on and training in system solutions to fix these issues. To address these issues, it is necessary to rely on and receive training in system solutions.

It is necessary to have extremely low latencies of 0.5–1 millisecond [6] to solve the problems described above and collect data at the same time. Because the latency in 4G networks is approximately 200 milliseconds, only 5G networks are currently capable of providing solutions for this range. A 5G network can connect up to one million devices per kilometer [7], and it has been demonstrated that a "5G frame structure" enables devices to share available 5G bandwidth even better through a combination of time and frequency division multiplexing [8], mitigating signal and radio interferences]. 5G networks can achieve speeds of up to 20 Mbps. One of the issues that currently exists with 5G is that there is a lack of industrial 5G equipment. However, over time, this issue will most likely be resolved within the next six months to one year. To satisfy this demand, manufacturers are not developing and producing on a large-scale new piece of hardware.

However, to overcome these obstacles, constraints, and issues, a distributed network infrastructure is required. This infrastructure must be able to deal with the outcomes of data integrity, coherence, and immutability. This is the reason why blockchain is thriving across industry. In a peer-to-peer network, blockchain operates as a shared, immutable ledger that not only records transactions but also keeps track of ownership and assets. Blockchain is a decentralized and distributed network. When a block is finished, the ledger entry for it can no longer be changed in any way.

## 2. Cybersecurity Current Overview

Digital system and infrastructure security, policies, and strategies have never been more important than now. Companies and governmental entities will spend $10.5 trillion yearly by 2025, up from $3 trillion USD in 2015 [9], where the global spending on cybersecurity products and services will be $1.75 trillion cumulatively for the five-year period from 2021 to 2025 [10].

Blockchain's main feature is a distributed ledger, which makes it more secure than both traditional distributed and centralized systems. This makes it harder for cybercriminals to act. The approach mitigates vulnerabilities by having a robust architecture (blocks) that records ownerships and transactions, ensuring integrity and data consistency. For instance, it reduces the chance of a single point of failure and makes it harder for hackers to break into the network. Similarly, once a block is added to the blockchain, it cannot be altered or deleted. This helps to ensure that the data stored on the blockchain is **tamper-proof** and can be trusted to be accurate. Because the ledger is spread across every node of the network, it increases the complexity and difficulty for hackers to compromise, steal, or delete data. It uses **cryptography** to secure the data stored on the network, which helps protect against unauthorized access and ensures that only authorized parties can view or modify the data. Encryption, either symmetric or asymmetric cryptography or cryptographic hashes, is built into the blockchain. This makes the architecture more robust. With the system's public keys and digital signatures, it can protect any kind of edge device. **Transparency**, meaning that all transactions can be viewed by anyone, makes it more difficult for malicious actors to hide their activities and makes it easier for network participants to detect suspicious activity. **Self-executing** contracts help reduce fraud and errors. Scale network security with consensus, which makes it hard for someone to take over the network. Also, the consensus algorithm prevents anomalies without the need for a centralized and hierarchical system. A recent study from Palo Alto Networks [11] says that: a) 98% of all IoT device traffic is not encrypted; b) 51% of threats to healthcare organizations involve imaging devices; and c) 72% of healthcare VLANs mix IoT and IT assets, while 57% of IoT

 doi:10.20944/preprints202306.1159.v1



devices are vulnerable to medium- or high-severity attacks and 41% of attacks take advantage of device vulnerabilities, making them an easy and desirable target for attackers. Blockchain technology eliminates the possibility of any form of distributed denial-of-service attack (DDoS) by not having a central point of access and by not being centralized.

## 3. Blockchains: Public and Private

There are public blockchains and private blockchains, and the distinction between the two is based on the amount of transparency that is provided. A public blockchain does not restrict who can participate, allows transactions to be verified in a way that is both transparent and decentralized, and is open to anyone who wants to use it. Bitcoin, Ethereum, and other cryptocurrencies come to mind as examples. On the other hand, a private blockchain is permissioned, which means that only participants who have been pre-approved can access it. When compared to public blockchains, these private blockchains are easier to scale and provide greater levels of privacy, but they are also less open and centralized. Organizations frequently make use of them for the purpose of maintaining their internal records and keeping tabs on their assets. Examples include Hyperledger, etc. The fifth industrial revolution makes the most of both blockchain types. Public blockchains provide a high degree of transparency while also being decentralized. This facilitates trust, security, and accountability among users. On the other hand, private blockchains provide an increased level of control in addition to increased levels of privacy, which makes them suitable for circumstances in which sensitive information needs to be protected.

Both types of blockchain need consensus mechanisms to make sure that the network is stable and safe. Consensus mechanisms are the ideas, protocols, and incentives that make it possible for a group of nodes in different places to agree on the state of a blockchain. According to the Oxford Dictionary [13], "consensus" refers to general agreement. There are different algorithms that are used to achieve consensus on the blockchain. Public blockchains use decentralized consensus mechanisms, in which several nodes compete to validate transactions. Regarding Ethereum, "blockchain" means that at least 66% of the nodes on the network agree on the global state of the network [12]. The fact that every node depends on the blockchain network is shown by the fact that everyone agrees on protocols, incentives, and ideas. On the other hand, private blockchains can use either centralized or decentralized consensus mechanisms, depending on the network's needs and goals. Most of the time, centralized consensus mechanisms are faster and more efficient, but they are less safe and easier to manipulate. Decentralized consensus mechanisms provide more security but are slower and less efficient.

The following subsection describes the various consensus mechanisms available for public and private blockchains.

### *3.1. Proof-of-Work (PoW)*

PoW is a consensus algorithm used to secure blockchain networks and validate transactions. Proof of Work (PoW) is the consensus mechanism used by Bitcoin, Litecoin, and Dogecoin. It was created by Satoshi Sakamoto, the creator of the Bitcoin blockchain. Ethereum until Ethereum 2.0 uses PoW. The idea behind PoW is that the puzzle is difficult to solve but easy to verify. The proof-of-work involves scanning for a value that, when hashed, such as with SHA-256, begins with a number of zero bits. The average amount of work needed grows by a factor of the number of zero bits needed, and this can be checked by running a single hash. The average amount of work needed grows by a factor of the number of zero bits needed, and this can be checked by running a single hash. For our timestamp network, we do the proof-of-work by increasing a nonce in the block until we find a value that gives the block's hash the required zero bits. [14] When the block meets the hash requirement of zeros, the block is “chained” to the network and can no longer be edited. The consensus convinces attackers that if they try to change a block, they will have to redo the proof of work for the existing block in the chain of blocks and, if they do that, they will have to redo other blocks as well. The system gives users bitcoins, whose value has been going down over time, when they find a mistake. So, centralization could happen if some users are rewarded more than others, which would favor the

 doi:10.20944/preprints202306.1159.v1



computing power of the rewarded users. And centralization may compromise data integrity. PoW is the most prevalent consensus mechanism for modeling public blockchains in general. Proof of Work (PoW) isn't usually used in private blockchains because it was made for public blockchains, which need decentralized consensus and protection from bad actors. Ethereum Classic is a private version of Ethereum that uses PoW consensus.

PoW has been an important part of the blockchain industry since the beginning, but it hasn't done much for Industry 5.0. PoW is hard to use for integrating advanced technologies because it uses a lot of energy, is hard to scale up, and could become centralized.

### *3.2. Proof-of-Stake (PoS)*

Proof of Stake (PoS) is an alternative to Proof of Work (PoW) that was implemented to address the shortcomings of PoW. PoS is better for the environment and uses less energy than PoW because it doesn't require miners to solve hard math problems to verify transactions. In PoS, the validation of transactions is carried out by validators, who are selected based on the amount of cryptocurrency they hold in the network. This is why PoS is also referred to as "staking." Because they have a stake in the network, the validators have a reason to check transactions honestly. If they check transactions with bad intentions or if the network is attacked, they could lose the tokens they staked. The process starts with a proposer, then a proposed block, and finally the validation of the proposed block [15]. The amount of cryptocurrency a validator has in the network affects how likely it is that they will be chosen as a validator. Bigger tokens' ownerships have more chances to be selected, even though the selection is random. Since there is no reward for mining, it encourages more nodes to take part in creating and validating blocks, which saves energy. In PoW, the validation process becomes more difficult as the network grows, which slows down the process of validating transactions. In PoS, the validation process remains constant, regardless of the size of the network. This makes it a more scalable solution, especially for blockchain networks with many users. The PoS is not without its drawbacks. One of the main criticisms of PoS is that it is vulnerable to the "nothing at stake" problem. In this case, validators have no reason not to switch to a different chain if a new chain with better rewards is made. This can lead to a situation where the original blockchain becomes vulnerable to attack. Despite being a "fairer" mechanism, it still has flaws for individuals with lower holdings, because ownership is correlated with the likelihood of selection, increasing the potential for centralization. Again, the mechanism may compromise decentralization, having in mind that smaller networks are less efficient at staking, leading the network for centralized nodes. PoS is used in both public and private blockchains. Ethereum (as of Ethereum 2.0), Cosmos, Tezos, Algorand, EOS, etc. are some public blockchain that make use of this consensus. Hyperledger Besu, Corda, Quorum, Chain Core, etc. are examples of private blockchain.

Proof of Stake has several advantages that make it well-suited for contributing to Industry 5.0, including its energy efficiency, scalability, and decentralization.

### *3.3. Delegated Proof-of-Stake (DPoS)*

DPoS relies on a select group of individuals, known as "delegates," or “witnesses”, who are responsible for achieving consensus during the block validation [16] to validate transactions. These delegates are elected by the community, and they are incentivized to act in the best interest of the network by being rewarded with transaction fees. The block validation is subject to a voting system by stakeholders to choose the external validator. The key difference between DPoS and other consensus mechanisms is that DPoS uses a democratic voting process to select its delegates. This process allows for a more efficient and secure network, as it eliminates the need for large amounts of computational power to validate transactions. One of the major benefits of DPoS is its ability to process transactions at a much faster rate than other consensus mechanisms. This is because DPoS networks have a much smaller number of delegates who are responsible for validating transactions, which allows for a more streamlined process. DPoS networks are also more scalable than other consensus mechanisms. This is because the number of delegates can be adjusted to meet the demands of the network, which means that the network can continue to grow and process more transactions

without sacrificing its speed or security. This mechanism promotes energy efficiency, but it may lead to further centralization and questionable ethical behavior because blockchain-based validation can stifle the spread of public opinion due to the limited number of delegates. Nonetheless, cases may force the mechanism to rely on centralized processes because a small number of token holders can impact and influence networks. DPoS is used in both public and private blockchains. EOS, Ark, TRON, BitShares are some examples of public blockchains that use this consensus. Hyperledger Iroha, Symbiont, Eris Industries are some examples of private blockchains that use this consensus.

Delegated Proof of Stake has several advantages that make it well-suited for contributing to Industry 5.0, including its fast block times (speed), low latency, efficiency, scalability, and decentralization.

### *3.4. Byzantine Fault Tolerance Family (BFT)*

The BFT is the feature of a distributed network to reach consensus (agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information [21]. It aims to protect the system against failures by employing collective decision making on correct and incorrect nodes, – this enables reduction on faulty nodes. The concept is inspired by the well-known Byzantine Generals' Problem [22]. The problem represents several Byzantine divisions, each led by a general and stationed outside an enemy city where generals can communicate via message. Before they take any action, they must agree on a common strategy. However, some generals are not trustworthy, and they will try to avoid loyal generals to reach an agreement. Facing this problem, generals must decide what to do, based on a strong majority of generals to have a common attack plan at the same time. The generals must have an algorithm to ensure that loyal generals decide the same action against the minority of the not trustworthy generals' bad plan. Finally, untrustworthy generals may carry out the bad plan without causing any harm because the majority of loyal generals carry out the same strategy at the same time, meeting a reasonable plan and agreement.

In conclusion, an agreement problem can be solved if at most n processors are faulty, which means that strictly more than two-thirds of the total number of processors should be honest, if we have 3n+1 working processors, allowing tolerance for n faults [22].

The consensus mechanisms are based on the BFT concept, different approaches, although they all rely on three key properties: (1) safety, (2) liveness and (3) fault tolerance. (1) A consensus protocol is determined to be safe if all nodes in the network agree on the same state of the blockchain. This means that the network will always reach consensus and all nodes will have the same view of the blockchain, even in the presence of network partitions or other failures. This is also referred to as the "consistency" of the shared state. (2) A consensus protocol guarantees liveness if all non-faulty nodes participating in consensus eventually produce a value, meaning the network can continue to operate even in the presence of failures or other issues. (3) A consensus protocol provides fault tolerance if it can recover from the failure of a node participating in consensus. This is done with the help of redundancy, finding and fixing errors, and other methods [23]. BFT algorithms are designed to ensure that the network can reach consensus even in the presence of failures, and that the network continues to operate even in the presence of network partitions or other issues. The BFT concept is widely used in distributed systems.

BFT has some limitations like (1) Scalability, (2) Latency and (3) Resource consumption. (1) BFT algorithms need a lot of messages to be sent between network nodes, which can make it harder for the network to grow as the number of nodes goes up. (2) BFT algorithms can also be slow, with high latency between nodes in the network. This can result in slow transaction processing times and a less responsive network. (3) BFT algorithms can use a lot of resources, like a lot of processing power, memory, and network bandwidth. This can limit the deployment of BFT algorithms in resource-constrained environments.

To overcome BFT limitations, the PBFT algorithm was developed. PBFT is a modification of BFT that aims to make consensus in a blockchain network more scalable, efficient, and useful. PBFT uses a pre-consensus protocol to reduce the number of messages sent between network nodes. This helps improve scalability and reduce latency. Also, PBFT uses a more efficient way to reach consensus. This

makes the network use less resources and lets it work in places where resources are limited. PBFT assumes that nodes may act maliciously and tries to overcome this by using a majority agreement mechanism, where the majority of nodes must agree on a single value. This helps to ensure that the network reaches consensus on a correct value, even in the presence of malicious nodes [17]. PBFT relies upon a combination of digital signatures, cryptographic hash functions, and majority agreement to ensure the authenticity and integrity of the data exchanged between nodes and to reach consensus on a correct value.

Like pBFT, the BFT comprises multiple other implementations like: (1) iBFT, (2) dBFT, (3) Tendermint, (4) mBFT (5) fBFT (6) DiemBFT etc.

(1) Istanbul BFT, also known as iBFT, is intended for use in large networks containing thousands of nodes. It uses a committee-based approach to reach consensus, where a group of nodes are selected to reach consensus. It is used in private blockchain networks. For example, iBFT is used with Quorum, Pantheon, etc.

(2) Delegated Byzantine Fault Tolerance or dBFT is designed to handle malicious nodes in the network and ensure the authenticity and integrity of the data being exchanged between nodes. dBFT is a combination of the Delegated Proof of Stake (DPoS) and Byzantine Fault Tolerance (BFT) algorithms, which means it offers scalability and high performance like DPoS, and the security and reliability of BFT. In dBFT, token holders vote for a set of nodes to act as bookkeepers, who then reach consensus on the next block in the chain using a BFT consensus mechanism. When compared to other BFT consensus algorithms, dBFT is known for being fast and having low latency. It is used in public blockchain networks. For example, NEO.

(3) Tendermint uses a leader-based approach to reach consensus, where a main node acts as the leader and is followed by backup nodes. Tendermint is known for its fast finality and low latency compared to other BFT consensus algorithms.When compared to other BFT consensus algorithms, Tendermint is known for being fast and having low latency. It is used in both public and private blockchain networks. For example, the Cosmos network, a decentralized public network of independent blockchains, and Binance Smart Chain, a decentralized private network.

(4) Modified Byzantine Fault Tolerance or mBFT, is also designed to improve its performance and scalability. mBFT uses a combination of digital signatures, cryptographic hash functions, and message broadcasts to reach consensus on the next block in the chain. Unlike traditional BFT algorithms, mBFT uses a simpler communication protocol and relies on a smaller number of nodes to reach consensus, making it more efficient and scalable. Despite its improved performance, mBFT still maintains the security and reliability of traditional BFT algorithms. It is used in private blockchain networks. For example, Hyperledger Besu.

(5) Fast Byzantine Fault Tolerance or fBFT is optimized for fast block confirmation times and high transaction throughput, making it ideal for decentralized systems that require quick, reliable transaction processing. It is used in private blockchain networks. For example, Chain network.

(6) DiemBFT is directly based on PBFT and indirectly based on BFT and aims to provide a stable, secure, and scalable platform for digital transactions and financial applications. It is based on the HotStuff [1] protocol, built on pBFT and aims to increase efficiency by reducing the number of messages and, thus, communications between nodes, while maintaining pBFT security and efficiency. The leader has a bigger role, rather than interaction between nodes. Security is improved because a leader is selected randomly (the leader/follower concept). Members are assumed to be nodes, and transactions are sent to them by clients, operating through a shared mempool [19]. A rotation rule allows nodes to become leaders, based on HotStuff, with controlled timeouts, and can propose new blocks to be added to the chain that must be approved by followers. When a block gets a voting majority, it is added to the chain and gets a "quorum certificate" which is spread across the network for validation. If the process goes well, it is stored in the chain. This allows the consensus to be faster at a minimum cost: compared with 7 transactions per second, the DiemBFT consensus allows 1000 per second. Although speed and efficiency features exist, there are some problems with security,

[1] https://arxiv.org/pdf/1803.05069.pdf

integrity, and privacy. Nevertheless, there is a centralized consensus. It requires power to compute because nodes must commit at least $10 million in Diem stable coins to participate. This consensus is used with Diem and Facebook's Libra. It is used in private blockchain networks. For example, Diem Blockchain.

Comparing iBFT with PBFT we know iBFT is more scalable than PBFT and has faster finality compared to PBFT. Instead of "leaders" and backup nodes, iBFT uses "proposers" who act like leaders and "validators," who act like backup nodes – they can validate blocks but have no active role on the consensus protocol. In each round, validators may choose a new proposer responsible for adding the next block for validation. The biggest difference between pBFT and iBFT is that in iBFT validators can change, while in pBFT they are static, which means, by principle, that in iBFT validators are more truthful and involved. Like other consensus mechanisms, pBFT and iBFT operate where malicious nodes don't exceed 66% of all nodes and block states do not require confirmation like they do on public consensus mechanisms (trust is assumed in private mechanisms). Also, compared with the public consensus, pBFT and iBFT consume less energy, taking into account the inexistence of minors to solve mathematical operations. Because they use a large number of messages to keep track between blocks and collective decisions, these consensus systems work better with a limited number of nodes. More nodes, imply more actions to be done. Even though pBFT and iBFT are still vulnerable to attacks and compromise security, a node may be attacked, and the leader may manipulate other nodes. Because of the leader/proposer, consensus allows nodes to be controlled in a closed system, different from public consensus mechanisms where nodes are open and free.

### *3.5. Distributed Proof of Security (dPoSec)*

The dPoSec consensus algorithm was developed with the goal of simplifying the operation of the blockchain network during communication and increasing the amount of work that can be done in a given amount of time[21]. It intends to function in a highly secure mode while also scaling itself towards a Phase-3 solution, which will make it a significant step forward in the field of blockchain consensus algorithms.

In order to provide a blockchain solution that is both quick and scalable, the dPoSec algorithm combines the most beneficial aspects of the Proof of Stake (PoS) protocol and the Byzantine Fault Tolerance (BFT) protocol. It incorporates advanced security measures that are based on trust establishment among nodes to ensure a fast, scalable, and secure network operation. It is a significant improvement over traditional consensus algorithms and represents a significant step forward in the evolution of consensus algorithms.

Because the dPoSec is built on the Ethereum Virtual Machine (EVM), it is able to execute all smart contracts and offers a flexible platform for the development of decentralized applications. This makes it possible for developers to build a diverse set of decentralized applications on the platform. Because of this, it is a flexible solution that can be implemented in a variety of fields, including the healthcare industry, the financial sector, and others.

dPoSec is a well-rounded and versatile platform because, in addition to its robust security features, it also provides on-demand privacy and efficient peer-to-peer discovery. This makes it an ideal solution for any situation. The algorithm was developed to be extremely scalable, and its architecture makes use of sophisticated blockchain primitives to improve both its performance and its efficiency. dPoSec's blockchain primitives are designed to be more efficient than those of other blockchains, which results in a number of benefits, including a reduction in the amount of time needed to process transactions and an increase in scalability. Because dPoSec is an on-demand privacy platform, users are able to protect the confidentiality of their data and take advantage of the privacy benefits that come along with using the service. This means that users can choose which information they want to share and with whom, giving them full control over their data and giving them the ability to make informed decisions. The peer-to-peer discovery feature of the platform makes it easy for nodes to find each other and establish connections, thereby lowering the network's latency and increasing its overall efficiency.

One of the most significant obstacles that blockchain networks must overcome is the requirement for a high level of coordination and communication between nodes. This can make the network move more slowly and raise the likelihood of it failing altogether. dPoSec is able to circumvent this difficulty by employing a one-of-a-kind validator selection process. This method was developed with the intention of lowering the likelihood that malicious actors will compromise the network and raising the level of network security overall. In order to maintain the reliability and safety of the network, validators are chosen using a variety of criteria, including the amount of stake they hold, their reputation, and their performance.

dPoSec makes use of a sophisticated reward mechanism for validators in order to ensure that the network's integrity is preserved and to thwart any attempts by malicious actors to compromise it. This incentivizes good behavior and punishes malicious actors, helping to maintain the network's security. The algorithm also eliminates the danger of "nothing at stake" attacks, which occur when validators carry out malicious behavior without fear of any repercussions as a result of their actions. dPoSec addresses this issue through its punishment mechanisms, which penalize malicious validators and incentivize good behavior.

dPoSec is a more secure and reliable consensus mechanism because it uses advanced security measures to increase trust in the running nodes. These measures include cryptographic signatures and consensus algorithms, among other things. This ensures that the network is protected against a variety of attacks, including those that exploit vulnerabilities in the consensus algorithm. This also protects the network from being compromised. For example, the utilization of cryptographic signatures helps to ensure that the network's integrity is maintained even in the event that one or more of its nodes are breached.

dPoSec was developed with a particular emphasis on security, efficiency, and scalability in order to cater to the requirements of a wide range of sectors and assist those sectors in maximizing the potential of blockchain technology. The algorithm is extremely adaptable and can be tailored to the particular requirements of each sector, which enables it to function as a solution that is both versatile and scalable. For instance, it can be used in the financial sector to ensure the safety and efficacy of payment transactions, and it can also be used in the healthcare sector to secure and manage electronic medical records. Both of these applications can be found in the financial sector. It is designed to meet the needs of a variety of industries and to assist those industries in making use of the benefits offered by blockchain technology. It accomplishes this by combining advanced security measures with a focus on scalability [21].

Both public and private blockchains are compatible with and capable of using dPoSec. This consensus is used by the Naoris Protocol, which is a hybrid public-private blockchain as per the end need.

dPoSec can contribute significantly to Industry 5.0 by offering a reliable and effective consensus mechanism for industrial blockchain applications. For instance, it can be used to safeguard the accuracy of information gathered from Internet of Things devices in a supply chain management system or to safely track the flow of goods through the supply chain.

### *3.6. Proof of Elapsed Time (PoET)*

PoET is designed to address the problem of energy waste in Proof of Work (PoW) and Proof of Stake (PoS) systems. The main goal of this consensus is to reduce energy consumption. Each node in the network waits for a random amount of time before it can participate in block validation. This waiting time is verified by a trusted entity, called the "Validator," who verifies that the node indeed waited for the specified time. Developed by Intel, the consensus enables a tool to solve the problem of selecting randomly a leader who makes decisions about mining permissions and block winners, aiming to spread winnings across a large number of participants [20]. By managing waiting times, managing energy consumption, the shortest randomly waiting time generated by a node wins the block. The consensus is fairer because it promotes a way of rewarding centralization and random leader selection, thus, the consensus remains probabilistic instead of deterministic. Hyperledger Sawtooth uses this consensus.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 June 2023 doi:10.20944/preprints202306.1159.v1



PoET can be used in both public and private blockchain networks. Hyperledger Sawtooth is a public blockchain that uses this consensus. Intel SGX is a private blockchain that uses this consensus.

*3.7. Proof of X (PoX)*

Revolutionary change is often accompanied by growing pains, and the world of blockchain technology is no exception. As the field continues to evolve, new problems arise and demand new solutions. One such area of innovation is the development of many such consensus algorithms and discussing them all will be out of scope for this version. There is currently more than 70+ different consensus algorithms that support either public or private blockchain networks, or both, and the list is constantly growing [55]. Some of the other most popular Proof-of-X algorithms include:

- Proof-of-Capacity/Space
  - This consensus algorithm uses disk space instead of computational power to validate transactions. The idea is that disk space is cheap and readily available, making it a more sustainable and energy-efficient alternative to PoW.
- Proof-of-Burn
  - This consensus algorithm requires users to "burn" tokens by sending them to a public address with no known private key. This reduces the supply of tokens in circulation, making it more difficult for attackers to accumulate a large amount of tokens to launch an attack.
- Hybrid models:
  - As the name suggests, hybrid models combine two or more consensus algorithms to take advantage of their strengths and mitigate their weaknesses. For example, a hybrid of PoW and Proof-of-Stake (PoS) might use PoW to secure the network against attacks, and PoS to validate transactions.
- Directed Acyclic Graph (DAG):
  - A DAG is a type of data structure that can be used to create a distributed ledger. In a DAG-based blockchain, transactions are validated based on their position in the graph, rather than through a traditional consensus mechanism.

By constantly pushing the boundaries and exploring new solutions, the field of blockchain transaction's finality; if it uses probabilistic or deterministic algorithms; If participants have or do not have permission to join the network and contribute to its maintenance [24]; The use of token need to operate; the scalability capacity in order to grow the network; Transaction speeds classification; Any costs of participation in infrastructure, computing power, operations in, or on the network; Energy efficiency; Trustiness regarding network trust to processes and transaction independently from participants and entities; Resilience to maintain a stable and common state across blocks; If decentralization is well implemented or not; Allowed tolerance in order to decisions and validate blocks; If decentralization, security and scalability are addressed, at least theoretically, known as blockchain trilemma; The layer type of blockchain, type 1, base layer, type 2, blockchains built in base layers type 1 and type 3, decentralized blockchains and protocols.

**Table 1.** Consensus mechanisms comparison.

| | Proof-of-Work (PoW) | Proof-of-Stake (PoS) | BFT Family (BFT) | Distributed Proof of Security (dPoSec) | Proof of Elapsed Time (PoET) |
|---|---|---|---|---|---|
| **Public** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** |
| **Transaction Finality** | **Eventually** | **Immediate** | **Immediate** | **Immediate** | **Immediate** |
| **Permissionless** | **Yes** | **No** | **No** | **No** | **Yes** |

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 June 2023 doi:10.20944/preprints202306.1159.v1



| Token | Generally used to reward participating nodes | Used to elect delegates | Not typically used | Generally used to reward participating nodes | Not typically used |
|---|---|---|---|---|---|
| Scalability | Low | High | Low | High | High |
| Security | High | High | High | High | High |
| Speed | Slow | Fast | Fast | Fast | Fast |
| Costs of Participation | High (electricity) | Low | Medium | Medium | Low |
| Energy Efficiency | Low | High | High | Medium | High |
| Trustiness | High | Medium | High | High | High |
| Resilience | High | High | High | High | High |
| Decentralization | High | Low | Low | Medium | High |
| Tolerance to Validation | Medium | High | High | Medium | Medium |
| Blockchain Trilemma | Weak in terms of scalability and energy efficiency | Stronger in terms of scalability and speed than PoW and PoS but weaker in terms of | Stronger in terms of security and speed than PoW and PoS but weaker in terms of scalability and decentralization | Varies based on implementation | Stronger in terms of energy efficiency and decentralization than PoW and PoS but weaker in terms of scalability |
| Layer 1/Layer 2 | Layer 1 | Layer 1 | Layer 1 | Layer 2 | Layer 2 |

*3.8. Discussion*

As expected, there is no "magic" consensus for all scenarios at sight, services, or industries. Issues such as the size of the infrastructure, the expected time of interactions, the classification of participants, the data to be exchanged, and so on must be addressed. Nevertheless, there are some considerations to keep in mind such as energy efficiency, decentralization, security of actions and transactions, the expected growth of devices, always keeping some guidelines in mind for achievement, business success, and costs. Trust, resilience, and tolerance are properties that should help on a decision of consensus to adopt. This should also be planned according to technologies that are available to organizations and infrastructures, where the consensus mechanism is the very heart of every blockchain solution [25]. Ultimately, any choice about the adoption of a blockchain solution

 doi:10.20944/preprints202306.1159.v1



should be made with a focus on the consensus process that underpins the solution and with a comprehensive grasp of the technologies and infrastructures that are currently accessible.

## 4. Industry 5.0 and Edge Computing

The digitalization of industry is an ongoing process, also known as Industry 5.0. Since automation, this is, probably, the most important stage of all times, with the aim for better management and optimization of all aspects of manufacturing processes and supply chain. Like Harald Lesch said, digitalization is the purest form for monetizing time [26] - to achieve this goal, there are a set of technologies and systems needed such as sensors, 5G networks and, at the core, robust distributed systems to gather and process all data. As presented previously the growth of sensors for different purposes is exponentially growing, while prices drop continuously. But, to make use of all end-of-line devices there is needed computers to gather and store all the data they transmit (1), process all the data in a way for achieving knowledge, validation and refine decisions in the supply chain (2) and, nevertheless, do it in the smallest time frame window that can be got (3) with the smallest amount of energy needed.

Companies like Bosch [27], Airbus [28] or BMW [29] have now implemented 5G networks in their production lines with the aim of gathering data to improve efficiency. Along with secure and reliable communication another important aspect is to achieve high-speed communication.

To get results from 5G, the use of remote servers in an edge computing architecture can provide greater power flexibility and overall process performance, resulting in lower implementation costs and greater sustainability. In an edge computing architecture, kilometers of cables are not required to connect sensors to communicate with control systems.[27]. Let us proceed to a briefing on Edge computing enhancements.

### *4.1. Edge Computing Enhancement for Industry*

Edge computing is a distributed computing paradigm that allows data processing to occur closer to the source of data, rather than in a centralized location. The main goal of edge computing is to reduce the amount of data that needs to be sent to centralized data centers, which can improve the speed and reliability of data processing, as well as reduce the costs associated with data transfer and storage.

It is expected that the edge computing market size is projected to reach USD 101.3 billion by 2027, at a CAGR of 17.8% [30], from components to applications. In a comparison study between cloud computing and edge computing [31], wireless networks are more suitable for sensor communications than wired networks for the cloud, and thus, more mobile implementation is desirable as well as greater scalability, allowing wider distribution of digital devices. Because of the reduction in cable, less power consumption is needed, reducing operational costs as well as storage costs. Other advantages are related to privacy and security, reducing data leakage during transmissions and also thanks to a decentralized network; low latency rates, enabling better data transmission and real-time results; more manageable data for analytics; and better interoperability thanks to the computing processing moving to the edge, which eliminates the need for device universal standards that are not yet defined.

Also, industrial process monitoring, and predictive maintenance are two of the most common use cases for edge computing implementation. Efficient communications across highly complex SCADA (supervisory control and data acquisition) systems to manage the high volumes of data from sensors and PLCs (programmable logic controllers) and the ability to track a variety of metrics and monitor the performance of machinery is becoming a standard in state-of-the art factory plants [32].

## 4. The “New Industry” Challenges

The new industrial revolution, also known as Industry 5.0, has significantly improved technology and changed how various industries function. Despite all of its advantages, Industry 5.0 has also created important challenges that must be overcome for successful adoption.

 doi:10.20944/preprints202306.1159.v1



Standardization, which is essential for seamless communication and collaboration across many platforms and systems, is one of the main issues. Latency, or the delay in data transport, is another important restriction that presents a problem for real-time applications. Additionally, to guarantee the secure and effective functioning of Industry 5.0 technologies, security, scalability, and dependability are significant challenges that must be addressed. For Industry 5.0 to reach its full potential and for industries all around the world to experience sustainable growth, it is essential to address these obstacles.

## 5. Major Challenges in Blockchain Adoption

### *4.1. Devices Incompatibility*

The adoption of blockchain in low-end IoT devices is challenging due to their limited processing power, memory, and energy resources. Low-end IoT devices may struggle to perform complex blockchain computations, resulting in slow transaction processing times and overall system performance degradation. These limitations make it difficult to adopt blockchain as a direct solution for Industry 5.0 legacy-based systems that rely on low-end IoT devices. Therefore, careful consideration must be given to the performance requirements of blockchain solutions and the capabilities of low-end IoT devices when implementing blockchain in Industry 5.0 applications.

### *4.2. Scalability*

The massive amount of data produced by numerous linked devices presents a significant challenge for blockchain technology. Blockchain is known for being slow and not scalable, potentially causing a bottleneck in the adoption of devices in Industry 5.0 systems. As a result, implementing blockchain in Industry 5.0 applications requires careful consideration of scalability issues to ensure efficient processing of vast amounts of data.

### *4.3. Interoperability*

The integration of Industry 5.0 devices with blockchain systems may be challenging due to the use of multiple protocols and standards that are incompatible with blockchain technology. The diverse range of protocols used in Industry 5.0 devices could potentially hinder the seamless integration of blockchain, making it difficult to establish effective communication and collaboration. Therefore, addressing interoperability issues is crucial for successful integration of Industry 5.0 devices with blockchain technology.

### *4.4. Security*

Although Industry 5.0 devices are generally considered secure, they may not be as secure as blockchain technology. The interconnectivity of devices in Industry 5.0 makes them vulnerable to security breaches, which could potentially compromise the integrity of the entire blockchain network. Therefore, ensuring the security of Industry 5.0 devices is critical to the successful implementation of blockchain technology in Industry 5.0 applications.

### *4.5. Privacy*

Industry 5.0 devices often collect sensitive data, which must be protected to ensure the privacy of individuals. Integrating blockchain with IoT requires careful consideration to ensure that data privacy is not compromised. Robust security measures must be put in place to safeguard sensitive data from unauthorized access and ensure the integrity of the blockchain network. Therefore, careful attention must be given to the privacy and security implications of integrating blockchain with IoT to ensure the successful implementation of Industry 5.0 applications.

### *4.6. Cost*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 June 2023 doi:10.20944/preprints202306.1159.v1



The integration of blockchain technology into an Industry 5.0 system can be a costly affair and may require significant investments in infrastructure, software, and hardware. The deployment of blockchain technology may require additional resources to support the increased computational demands and data storage requirements of the system. Therefore, implementing blockchain in Industry 5.0 applications requires careful consideration of the costs involved to ensure the feasibility of the integration.

### *4.6. Trustlessness*

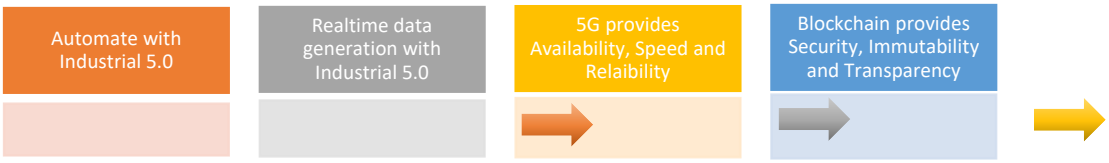
While trustlessness is a key benefit of blockchain technology, it also presents a significant challenge. While this eliminates the need for trust in centralized entities, it can create vulnerabilities in the system that malicious actors can exploit. One of the significant security challenges presented by trustlessness is the potential for 51% attacks. A 51% attack occurs when an entity gains control of over 50% of the computing power of the blockchain network. Furthermore, the absence of trusted intermediaries in a trustless system can also make it challenging to identify and address security breaches, as there is no central authority to oversee the transactions.

### *4.7. Storage*

Another significant challenge in adopting blockchain for devices is the issue of storage space. Industry 5.0 devices generate massive amounts of data, and recording all the data on the blockchain network can quickly exhaust the storage capacity of the devices. Moreover, storing large amounts of data on the blockchain can increase the overall size of the blockchain, making it less scalable and less efficient.

## 5. Gathering Blockchain and Edge Computing: A Proposal Distributed Computing Solution

While many blockchain solutions have been proposed to address various challenges, none of them resolve all the issues. As a result, the adoption of blockchain has been challenging, as individual blockchain solutions may not be sufficient to address all the problems. As a result, a set of components, devices, applications, architectures, and technologies may address challenges industry needs. As an example, Bosch Security Systems, S.A, located in the northern region of Portugal is now using more than 5000 5G sensoring devices to improve production on their products. The industry is using each day more sensors to collect data and process data to improve maintenance (predicted), reduce waiting times and produce more with higher cost-efficiency ratios. Although these changes, most of the processing is done with an edge-computing strategy, which means local processing, which is good for data privacy data and rapidness data analysis but cannot be integrated in a blockchain network.




As previously stated, dPoSec has been designed to address almost all the challenges discussed earlier and can play a crucial role in Industry 5.0. It offers a customized EVM based robust and efficient consensus mechanism designed with security first approach for industrial blockchain applications and can be utilized to ensure the accuracy and reliability of information gathered from Internet of Things (IoT) devices across various domains. By utilizing dPoSec, Industry 5.0 can benefit from enhanced security, scalability, and interoperability, making it easier to implement and manage complex blockchain solutions.

dPoSec is a consensus mechanism that combines the power of edge computing and local processing to establish trust and enhance the security of the blockchain network. By utilizing local processing power, dPoSec can provide IoT devices with the ability to participate in the consensus process, which enhances the security and efficiency of the network. Furthermore, dPoSec is designed to learn from the knowledge gained during network operation and to develop defenses for all

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 June 2023 doi:10.20944/preprints202306.1159.v1



associated devices. This enables the network to adapt and evolve, building confidence among devices and promoting collaboration. As a result, dPoSec can help to overcome some of the most significant challenges of Industry 5.0, such as scalability, interoperability, and security, making it easier to implement complex blockchain solutions.

By leveraging dPoSec, Industry 5.0 can benefit from an enhanced security posture that enables IoT devices to operate with greater trust and efficiency within the blockchain network. This can lead to improved data accuracy, faster processing times, and increased resilience against cyber-attacks. Ultimately, the combination of edge computing and local processing provided by dPoSec offers a reliable and effective consensus mechanism for industrial blockchain applications, helping to unlock the full potential of Industry 5.0.

You may have a blockchain network in the powerplant, gathering and controlling data across servers, desktops and tablets and you also may have sensors data in devices, gathering it for local processing in the form of edge-computing. But the two worlds don't exchange information.

Our proposal is the integration of dPoSec protocol as blockchain network with sensoring devices, providing information for the blockchain network and edge-computer processing.

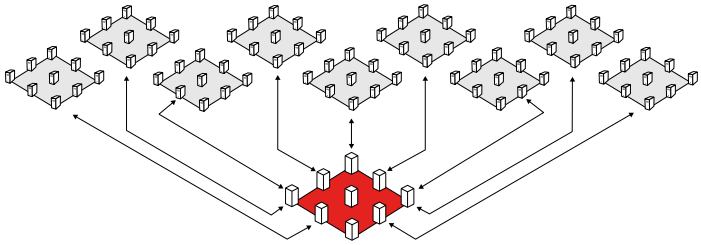


**Figure 3.** dPoSec blockchain networking view with a plethora of connected verge clusters and their separate meshes. Each mesh may be composed of several IIoT sensors with blockchain firmware.

To address challenges, sensors and machinery, performing data acquisition for posterior edge processing, need to be prepared to support the upload of blockchain firmware. Despite the fact there are several manufacturers that support this technology, most of them are proprietary and closed solutions. dPoSec based network comprises of:

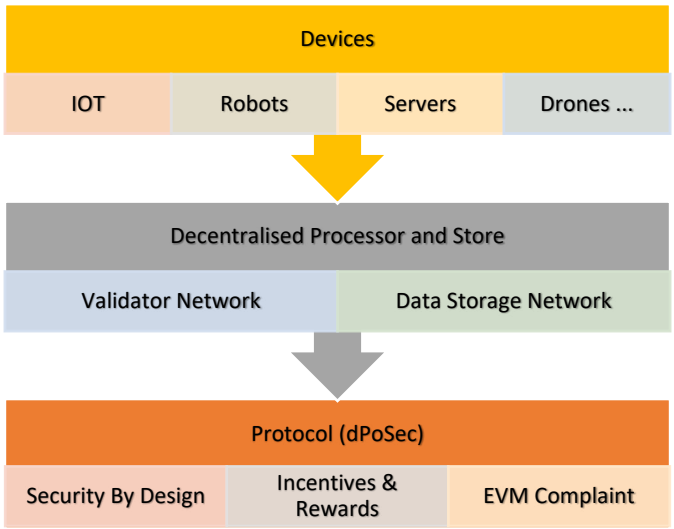



**Figure 4.** dPoSec blockchain upload process.

## 5. Conclusions

As a result, a set of components, devices, applications, architectures, and technologies are now available to drive industry digitalization and efficiency while addressing new challenges. The

touchstone at the present moment must be the integration of these built-in simple use cases and their spread over the shop floor.

The digitalization of industry is an ongoing process, also referred to as Industry 5.0., involves the use of advanced technologies such as artificial intelligence, robotics, IIoT, cloud computing, virtual reality, augmented reality and blockchain. It is transforming how organizations operate from production to customer service, enabling the integration of data from a variety of sources and helping in the automation of processes. It is also reducing the need for human resources and increasing the efficiency of many organizations [33]. The use of digital technologies has enabled companies to optimize their operations and create new products and services that are more personalized to customers [34]. Combining the discussed technologies will make improvements in supply chains and shop floors standard procedure.

Sensorization can provide greater accuracy and real-time data, allowing for more informed decisions to be made in real-time. Blockchain consensus can help to provide a secure, trustless, and immutable platform for data and transactions, eliminating the need to verify transactions through a centralized authority. Edge computing can reduce latency and increase data processing speed, allowing for quicker decisions to be made and for more complex tasks to be performed. 5G can provide faster internet speeds and increased bandwidth, allowing for more data and devices to be transmitted and processed faster. Overall, the combination of these technologies can offer organizations and individuals greater efficiency, security, transparency, and cost savings.

Also, edge computing and blockchain complement each other, they are not inherently similar. Edge computing can also optimize the performance of blockchain-based systems by reducing latency and improving response times.

Nevertheless, challenges and constraints arise for companies when facing new outcome standards: Lack of knowledge and expertise: Companies may lack the knowledge and expertise to implement Industry 5.0 technologies, making it difficult to take advantage of the benefits they offer (1)[35]; High cost of implementation: Implementing Industry 5.0 requires significant capital investment in expensive technologies, such as artificial intelligence, robotics, and Internet of Things (IoT) systems (2)[36]; Security risks: Connecting systems and data to the Internet creates potential security risks, and companies must invest in security measures to protect their data and networks(3)[37]; Adaptability and scalability: Companies must be able to quickly adapt to changing technologies and customer needs, which can be difficult for companies to do without the right infrastructure in place (4)[38]; Regulatory restrictions: Depending on the industry, there may be regulatory restrictions in place that limit the use of certain technologies, such as autonomous vehicles or drones (5)[39].

One of the key challenges in implementing edge computing is ensuring the security and privacy of the data that is being processed and transmitted. Data breaches and cyberattacks are becoming more and more likely as more gadgets are connected to the internet. Blockchain can fill this need by offering a safe and unhackable method of data storage and distribution. For example, a smart factory where hundreds of sensors are gathering information on the functionality of various machines and pieces of equipment. To enable predictive maintenance and other uses, this data must be analyzed in real-time, but it must also be secured to prevent unwanted access. The factory can guarantee that only authorized parties have access to the data and that any modifications or updates to the data are documented and confirmed by using blockchain to store and exchange this data.

Similarly, to enable safe and effective navigation, self-driving cars need to handle a lot of data in real-time, including data from cameras, lidar, and other sensors. The car can make judgments more quickly and react to changing situations in real-time if edge computing is used to process this data locally rather than sending it to a centralized cloud-based system. As the car is gathering information about its surroundings and the actions of other drivers, this also raises questions regarding data security and privacy. The automobile can make sure that only authorized parties have access to the data, that any modifications or updates to the data are recorded and confirmed, and that the data is securely stored and shared via blockchain.

Extending businesses surely increase the effectiveness and transparency by employing sensors and other IoT devices to monitor the movement and condition of their products and the data is securely stored and shared by using blockchain technology.

When combined, edge computing and blockchain—two of the most exciting and promising technologies of our time—offer a potent solution that can open up a wide range of new use cases and applications. Edge computing and blockchain are poised to disrupt numerous industries and how we live and work by enhancing data security and privacy, enabling new business models and revenue sources, and enhancing the efficiency and transparency of supply chains.

**Author Contributions:** For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used "Conceptualization, X.X. and Y.Y.; methodology, X.X.; software, X.X.; validation, X.X., Y.Y. and Z.Z.; formal analysis, X.X.; investigation, X.X.; resources, X.X.; data curation, X.X.; writing—original draft preparation, X.X.; writing—review and editing, X.X.; visualization, X.X.; supervision, X.X.; project administration, X.X.; funding acquisition, Y.Y. All authors have read and agreed to the published version of the manuscript.", please turn to the CRediT taxonomy for the term explanation. Authorship must be limited to those who have contributed substantially to the work reported.

**Funding:** Please add: "This research received no external funding" or "This research was funded by NAME OF FUNDER, grant number XXX" and "The APC was funded by XXX". Check carefully that the details given are accurate and use the standard spelling of funding agency names at https://search.crossref.org/funding, any errors may affect your future funding.

**Acknowledgments:** In this section you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

**Conflicts of Interest:** Declare conflicts of interest or state "The authors declare no conflict of interest." Authors must identify and declare any personal circumstances or interest that may be perceived as inappropriately influencing the representation or interpretation of reported research results. Any role of the funders in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript, or in the decision to publish the results must be declared in this section. If there is no role, please state "The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results".

## References

1. Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Shanay Rab, Rajiv Suman, Significance of sensors for industry 4.0: Roles, capabilities, and applications, *Sensors International*, **2021**, 2, 1-12
2. 2019 Manufacturing Trends Report, **2019**,. Available online: URL https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-Report-2019-Manufacturing-Trends.pdf (accessed on 8th November 2022)
3. Cost of a Data Breach Report **2021**, IBM, 2021
4. 2021, Statista, Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025, Available online: URL https://www.statista.com/statistics/871513/worldwide-data-created/ (accessed on 10th November 2022)
5. Larry Myler, Better Data Quality Equals Higher Marketing ROI, *Forbes*, **2017**, Available online: URL https://www.forbes.com/sites/larrymyler/2017/07/11/better-data-quality-equals-higher-marketing-roi/?sh=53fe05867b68 (accessed on 10th November 2022)
6. Dalimir Orfanus, Reidar Indergaard, Gunnar Prytz, and Tormod Wien, Ethercat-based platform for distributed control in high-performance industrial applications. *Proc. IEEE 18th Conf. Emerg. Technol. Factory Autom. (ETFA)*, pages 1–8. IEEE, **2013**.
7. Statista, Connection density of 4G, 5G, and 6G mobile broadband technologies, Available online: URL https://www.statista.com/statistics/1183690/mobile-broadband-connection-density/ (accessed on 10th November 2022)
8. GSMA, 5G for Industry 4.0 operational technology networks - A comparison of the features and application of 5G and Wi-Fi 6 for manufacturing, production and supply chain use cases, **2021**, Available online: URL https://www.gsma.com/iot/wp-content/uploads/2021/03/2021-03-GSMA-5G-Industry-4.0-Op-Tech-Networks.pdf (accessed on 21th November 2022).
9. Microsoft Secure Blog Staff, The Emerging Era of Cyber Defense and Cybercrime, **2016**, Available online: URL https://www.microsoft.com/en-us/security/blog/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/ (accessed on 22th November 2022).

10. David Braue, Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025, *Cybersecurity Ventures*, **2021**. Available online: URL https://cybersecurityventures.com/cybersecurity-spending-2021-2025/ (accessed on 22th November 2022)
11. Unit 42, *2020 Unit 42 IoT Threat Report*, **2020** Available online: URL https://unit42.paloaltonetworks.com/iot-threat-report-2020/ (accessed on 23th November 2022)
12. Luka Kropec, Paul Wackerow, Joshua, Joseph Cook, Sam Richards, Seth Ariel Green, Samarth Saxena, Bienvenido Rodriguez, Hayden Fowler, Corwin Smith, elshigori, Victor Luna, Don Cross, Patrick Collins, Ryan Cordell, Consensus Mechanisms, *Ethereum Development Documentation*, **2022**, Available online: URL https://ethereum.org/en/developers/docs/consensus-mechanisms/ (accessed on 24th November 2022)
13. Oxford English Dictionary, Second Edition, 1989
14. Satoshi Sakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, **2008**. Available online: URL https://bitcoin.org/bitcoin.pdf (accessed on 24th November 2022)
15. Luka Kropec, Paul Wackerow, Joshua, Joseph Cook, Sam Richards, Seth Ariel Green, Samarth Saxena, Bienvenido Rodriguez, Hayden Fowler, Corwin Smith, elshigori, Victor Luna, Don Cross, Patrick Collins, Ryan Cordell, Proof-Of-Stake, *Ethereum Development Documentation*, **2022**, Available online: URL https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (accessed on 25th November 2022)
16. Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, and Jayaprakash Kar, A Research Survey on Applications of Consensus Protocols in Blockchain, *Hindawi Security and Communication Networks*, **2021**, Volume 2021.
17. Parma Bains, Blockchain Consensus Mechanisms: A Primer for Supervisors, *Fintech Notes*, **2022**. Available online: URL https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022003.ashx/ (accessed on 25th November 2022)
18. Martin Florian, Sebastian Henningsen, Charmaine Ndolo & Björn Scheuermann, The sum of its parts: Analysis of federated byzantine agreement systems, *Distributed Computing*, **2022**, Volume 35, pages399–417
19. The Ontology Team, HotStuff: the Consensus Protocol Behind Facebook's LibraBFT, *Ontology Tech Point*, **2019**, Available online: URL https://medium.com/ontologynetwork/hotstuff-the-consensus-protocol-behind-facebooks-librabft-a5503680b151 (accessed on 25th November 2022)
20. Ghassan Karame, Michael Huth and Claire Vishik, An overview of blockchain science and engineering, *Royal Society Open Science*, **2020**. Available online: URL https://royalsocietypublishing.org/doi/10.1098/rsos.200168 (accessed on 26th November 2022)
21. David Carvalho, Sumit Chauhan, CyberSecurity Mesh HyperStructure for the Digital World, *Naoris Procotol*, **2022**.
22. Marshall Pease, Robert Shostak, Leslie Lamport, Reaching Agreement in the Presence of Faults, *Journal of the Association for Computing Machinery 27*, **1980** , Vol 2
23. Arati Baliga, Understanding Blockchain Consensus Models, *Persistent*, **2017**.
24. Freeman Law, Permissioned and permissionless blockchains. Available online: URL https://freemanlaw.com/permission-and-permissionless-blockchains/ (accessed 2nd December 2022)
25. Kwadjo Nyante, [EP -2 ] The Magic Behind Blockchain: ⇛ Partial Exploit ⇚, *Medium*, **2022**, Available online: URL https://medium.com/naoris-protocol/ep-2-the-magic-behind-blockchain-partial-exploit-42d511d5db7e (accessed 2nd December 2022)
26. Harald Lesch, So Much About Digital, *Netflix Documentary Series*, **2022**.
27. Bosch implementa rede local 5G para produção mais inteligente em Aveiro e Ovar, *Bosch Notícias e Histórias*, **2022**, Available online: URL https://www.bosch.pt/noticias-e-historias/2021/bosch-implementa-rede-local-5g-para-producao-mais-inteligente-em-aveiro-e-ovar/ (accessed 5th December 2022)
28. Airbus launches Airspace Link 5G Air-to-Ground broadband connectivity in China, *Airbus Aircraft Newsroom*, **2022**, Available online: URL https://aircraft.airbus.com/en/newsroom/news/2022-06-airbus-launches-airspace-link-5g-air-to-ground-broadband-connectivity-in (accessed 5th December 2022)
29. Intelligent connected factory with 5G technology: Autonomous logistics at BMW Group Plant Landshut calculates data in the cloud, *BMW PressClub Global*, 2022, Available online: URL https://www.press.bmwgroup.com/global/article/detail/T0396773EN/intelligent-connected-factory-with-5g-technology:-autonomous-logistics-at-bmw-group-plant-landshut-calculates-data-in-the-cloud?language=en (accessed 5th December 2022)
30. Edge Computing Market by Component (Hardware, Software, and Services), Application (Smart Cities, Remote Monitoring, IIoT, AR and VR, Content Delivery), Organization Size (Large Enterprises and SMEs), Vertical and Region - Global Forecast to 2027, Markets and Markets, **2022**, Available online: URL https://www.marketsandmarkets.com/Market-Reports/edge-computing-market-133384090.html?gclid=Cj0KCQiAyracBhDoARIsACGFcS4u9IrlmsvkM6lO-46_9MclyK7W47ujY4SsyN31ryb9k-Jy_D_PGZ8aAqMVEALw_wcB (accessed 5th December 2022)
31. Tie Qiu, Jiancheng Chi, Xiaobo Zhou, Zhaolong Ning, Mohammed Atiquzzaman, Dapeng Oliver Wu, Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges, *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, VOL. 22, NO. 4, FOURTH QUARTER 2020, **2020**.

32. Brandon Moser, Edge Computing Examples Across Vertical Industries, Digi Blog, **2022**. Available online: URL httos://digi.com/blog/post/edge-computing-examples-across-vertical-industries (accessed 5th December 2022)
33. Kumar, A., & Prakash, A. Impact of AI and Robotics on Human Resource Management. *International Journal of Advanced Research in Management and Social Sciences*, **2019**,8(2), 189-193.
34. Freeman, Richard B. The Use of Digital Technologies Has Enabled Companies to Optimize Their Operations and Create New Products and Services That Are More Personalised to Customers. *International Journal of Business and Economics*, **2017**, vol. 16, nº 1, p. 23-32.
35. Jha, R. Challenges of Industry 4.0: The lack of knowledge and expertise, **2019**. Available online: URL https://www.themanufacturer.com/articles/industry-4-0-challenges/ (accessed 19th December 2022)
36. Das, S. Top 4 challenges of the industry 4.0 revolution, **2020**. Available online: URL https://www.forbes.com/sites/forbestechcouncil/2020/01/15/top-4-challenges-of-the-industry-4-0-revolution/?sh=7d3c3d48e7a2 (accessed 19th December 2022)
37. Thalmann, N. What are the security risks associated with Industry 4.0?, **2020**. Available online: URL https://www.techrepublic.com/article/what-are-the-security-risks-associated-with-industry-4-0/ (accessed 19th December 2022)
38. David, S. & Ngo, M. (2020). The biggest challenges of industry 4.0, **2020**. Available online: URL https://www.manufacturingglobal.com/technology/biggest-challenges-industry-40 (accessed 19th December 2022)
39. Abboud, M. (2020). Challenges of implementing industry 4.0, **2020**. Available online: URL https://www.sapinsider.com/it-strategy/challenges-of-implementing-industry-4-0/ (accessed 19th December 2022)