Review

Not peer-reviewed version

Enhancing Decentralized Decision-Making with Big Data and Blockchain Technology. A Comprehensive Review

Leonidas Theodorakopoulos * , Alexandra Theodoropoulou , Constantinos Halkiopoulos

Posted Date: 25 July 2024

doi: 10.20944/preprints202407.1977.v1

Keywords: big data analytics; distributed systems; consensus mechanisms; decentralized systems; real-life case studies.

Review

Enhancing Decentralized Decision-Making with Big Data and Blockchain Technology. A Comprehensive Review

Leonidas Theodorakopoulos *, Alexandra Theodoropoulou and Constantinos Halkiopoulos

Department of Management Science and Technology, University of Patras, 26334 Patras, Greece; theodoropouloua@upatras.gr (A.T.); halkion@upatras.gr (C.H.);
* Correspondence: theodleo@upatras.gr

Abstract: Big Data and blockchain technology are coming together to revolutionize how decisions are made in a decentralized way across various industries. This review looks at how these technologies, along with distributed systems, can improve data security, transparency, and real-time processing, making decision-making more efficient and informed. The integration enhances data security with unchangeable records, increases transparency and traceability, and supports real-time data analysis. However, there are challenges to overcome, including scalability, data privacy, interoperability, regulatory compliance, and high costs. By examining case studies such as Estonia's healthcare system, IBM and Walmart's Food Trust, and the Brooklyn Microgrid project, we explore the practical applications and benefits of combining Big Data with blockchain. Despite these hurdles, the review finds that the ongoing advancements and innovative solutions in these technologies offer significant promise. They are set to drive the adoption and effectiveness of decentralized decision-making, ultimately leading to better efficiency and outcomes across multiple sectors.

Keywords: big data analytics; distributed systems; consensus mechanisms; decentralized systems; real-life case studies

1. Introduction

The integration of Big Data and blockchain technology is set to revolutionize decentralized decision-making across various industries. As the digital landscape continues to expand, the sheer volume and complexity of data generated necessitate robust and innovative solutions to manage, analyze, and secure this information. Blockchain technology, with its immutable ledger and decentralized nature, provides a secure and transparent framework for data storage and management. When integrated with Big Data analytics, it enables real-time processing and analysis of vast datasets, facilitating informed and efficient decision-making processes.

Blockchain technology was initially introduced in the aftermath of the 2008 economic crisis to address discrepancies in financial information and restore trust between the financial industry and its clients. The emergence of Bitcoin, the first virtual currency based on blockchain technology, demonstrated the potential of this technology beyond the realm of cryptocurrencies. Today, blockchain applications extend across various sectors, including healthcare, supply chain management, finance, and public administration, offering solutions for secure and transparent transactions, digital identity verification, and decentralized governance.

Big Data, characterized by the five V's – volume, velocity, variety, veracity, and value – refers to the massive amounts of data generated from various sources, including social media, IoT devices, and transactional systems. The ability to process and analyze Big Data in real time is critical for deriving actionable insights and supporting decision-making processes. However, the challenges associated with Big Data, such as data security, privacy, and integration, necessitate advanced technologies to ensure its effective utilization.

 doi:10.20944/preprints202407.1977.v1

Integrating Big Data with blockchain technology addresses these challenges by providing a secure, transparent, and decentralized framework for data management. Blockchain's decentralized nature eliminates the need for intermediaries, reducing the risk of data breaches and ensuring data integrity. The immutable ledger ensures that once data is recorded, it cannot be altered or tampered with, providing a reliable foundation for decision-making.

The combination of these technologies enhances data transparency and traceability, allowing organizations to track data provenance and ensure its authenticity. This capability is particularly valuable in industries such as supply chain management, where tracking the origin and journey of products is essential. Additionally, the integration supports real-time data processing and decision-making, enabling organizations to respond swiftly to emerging trends and threats.

Today, industries are increasingly adopting these integrated technologies to transform their operations. In healthcare, blockchain ensures the integrity of patient records while Big Data analytics enables personalized treatment plans. In supply chain management, blockchain's traceability combined with real-time analytics optimizes logistics and reduces costs. Financial services benefit from enhanced security and fraud detection through blockchain's immutable ledger and Big Data's predictive analytics. As these examples illustrate, the convergence of Big Data and blockchain is not just a theoretical concept but a practical reality that is reshaping industries and driving innovation.

Despite the promising potential of integrating Big Data and blockchain technology, several challenges and potential issues need to be addressed. Scalability, data privacy, interoperability, regulatory compliance, cost, resource allocation, and governance are critical areas that require careful consideration and innovative solutions. By addressing these challenges, organizations can create robust, efficient, and secure decentralized decision-making systems that leverage the strengths of both Big Data and blockchain technology.

This comprehensive review aims to explore the intersection of Big Data and blockchain technology, examining their integration's benefits, challenges, and real-world applications. Through detailed analysis and case studies, this paper provides insights into how these technologies can transform decentralized decision-making processes, driving innovation and improving outcomes across various sectors.

2. Overview of Blockchain Technology

Blockchain technology was initially introduced after the economic crisis of 2008. Because of this crisis, the main problem that was identified and needed to be addressed was the discrepancies that were noted in the information presented between the financial industry and its clients. Thus, emerged the term “FinTech”, which comes from the words “Finance” and “Technology” and utilizes blockchain, artificial intelligence and data capture and analysis [1].

The first virtual currency that made its appearance, based on blockchain technology, was the bitcoin. Although blockchain is the foundation of bitcoin’s cryptographic nature, it soon was applied to other industries as well [1]. The true number of blockchain’s applications has still not reached its limit, with e-voting and digital ID, cross-border payments, crowdfunding, secure and transparent transactions in the gaming industry, land registration databases and automation in insurance processes, including fraud detection, among many others.

Blockchain can be defined as a distributed database or a digital ledger that maintains and carries a list of records in the form of data blocks, in a chronological order, that keeps growing with each transaction being recorded in it [2]. When a transaction is being made, an asymmetric cryptographic digital signature is created, which is then used to validate and authenticate it. During this process, a set of keys is created; a public key and a private key, which are owned by the two participants making the transaction in that network. The public key, used in the decryption process, is visible to everyone and becomes known through the entire network, while the private key is only known to its owner, is used in the encryption of the transaction and in its decryption, and it is used to initiate and sign transactions in a secure way [2].

 doi:10.20944/preprints202407.1977.v1

2.1. Blockchain Features

Figure 1 depicts the 4 main characteristics of Blockchain technology.

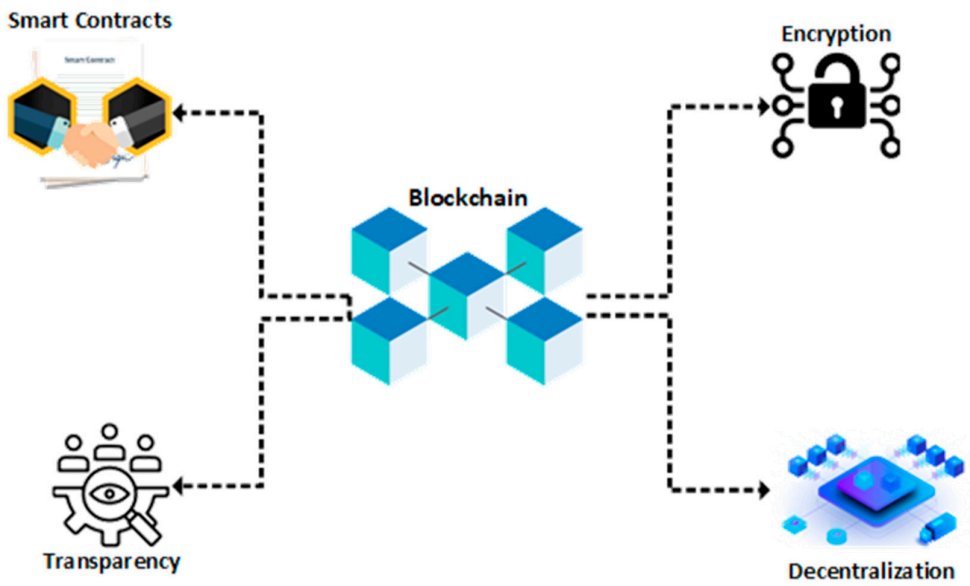

Figure 1. The 4 main features of Blockchain technology.

- Decentralization: In traditional centralized transaction systems, a third-party agency was always required in order to validate and authenticate each transaction being made between two parties. For example, a bank (central or commercial) would serve as a mediator in a every kind of transaction between two individuals. This would result in an overload to their central systems and servers. In blockchain, due to its utilization of consensus algorithms, third parties are no longer required to act as intermediaries, thereby giving blockchain its decentralized nature [3].
- Anonymity: Due to its decentralized nature, blockchain allows users to execute their transactions under entirely random generated addresses, since there is no centralized authority system to record, monitor and validate the authenticity of these addresses.
- Auditability (Transparency): In blockchain technology, a digital distributed ledger and a digital timestamp are used in order to record and validate each transaction. This means that whoever has access to any node in the network can trace and audit any previous record. In Bitcoin, for example, which is the first and most frequently used cryptocurrency, all transactions can be traced, thus making the data in the blockchain transparent and auditable [5].
- Immutability (Persistency): Once a transaction has been recorded in the blockchain, it cannot be tampered with or deleted by any party. This is one of many aspects that makes blockchain networks secure and easily trusted. It works like this; each block in the blockchain contains a unique piece of code, called a hash, which works like a digital fingerprint. When a new block is created, this hash consists of all the information inside the block, including details of the transaction being made, the hash from previous blocks and a timestamp, among other information. If anyone attempts to change any information in the block, the hash (fingerprint) will also change, thus signaling that someone has tried to alter something in the blockchain.

2.2. How Blockchain Technology Works

As mentioned previously, a private key is employed in order to initiate a transaction between two participants. Each transaction is added in a pool used by the technology to store all the transactions of the same network. The transaction contains details such as the sender's information and the receiver's address, the amount of data that is being transferred and a timestamp. Figure 2 visualizes in a simple way how Blockchain works.

 doi:10.20944/preprints202407.1977.v1

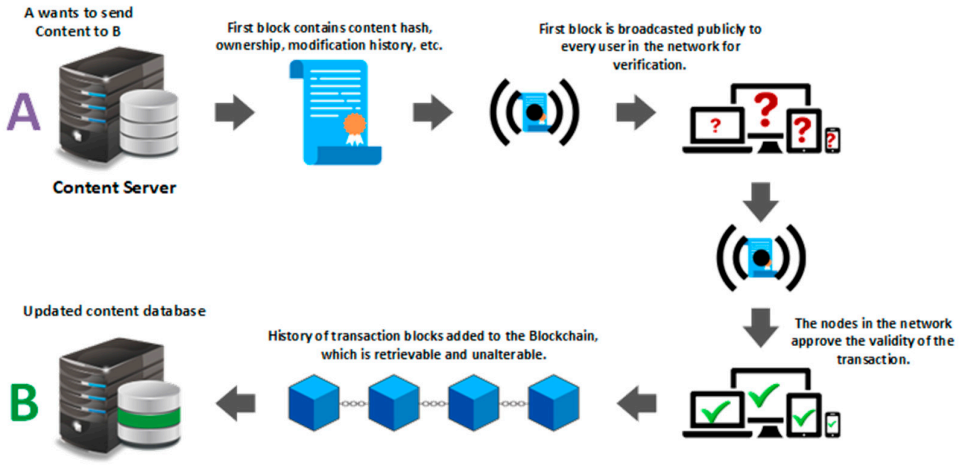

Figure 2. How Blockchain Technology works.

One of blockchain's major features is its anonymity, which is both an advantage and a problem for the technology. Both parties in a transaction have the need to remain anonymous. That, however, can have a negative impact on the trust between the users. This is why each and every transaction needs to be validated that it is indeed legal and then be put into a block. Thus, an agreement must be reached for the transactions to be put in said block to the blockchain. That can be achieved through consensus algorithms [5].

2.2.1. Consensus Algorithms

Consensus algorithms are mechanisms used in Blockchain so that all participants can reach a mutual agreement on the validity of the transactions being made, despite the fact that potential failures or inconsistencies might be discovered in the data. There are many types of consensus algorithms that have been developed, each with its own advantages and disadvantages as well as unique features. Reaching a consensus on blocks or transactions has proved to be quite challenging because these algorithms need to maintain a certain stability and resilience against node failures, corrupted or delayed messages and nodes that seem malicious or are unresponsive [6].

There are many types of consensus algorithms, the most important of which are summarized below:

2.2.1.1. Proof of Work (PoW)

Originally, Proof of Work was used by Bitcoin. It is like a game where all participants need to agree on a transaction record. Imagine a teacher in a classroom that hands out a quite challenging puzzle that requires time and effort in order to be solved. Once it is solved, however, it becomes easy for everyone to check if the answer is correct. In blockchain, miners or validators are the ones that compete with each other in order to solve a cryptographic puzzle and add a new block in the chain. This same process starts over for the next set of transactions (new blocks), making sure that the blockchain remains secure and agreed upon by all participants, without any need for intermediaries to act as a central authority. Figure 3 shows how the algorithm Proof of Work operates.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 25 July 2024 doi:10.20944/preprints202407.1977.v1

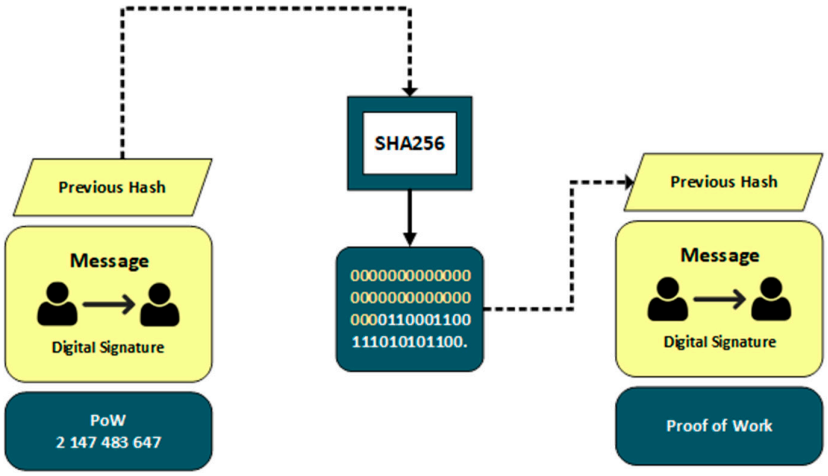

Figure 3. Proof of Work (PoW).

2.2.1.2. Proof of Stake (PoS)

Proof of Stake was developed as an alternative to Proof of Work. This algorithm, instead of solving a complex puzzle, works with a process of random selection, like a lottery system, plus in investment-like mechanism, in order to reach a consensus and validate transactions. In this algorithm, validators or stakers, place their own cryptocurrency as a stake, in order to prove that they are serious and trustworthy. Think of it as placing a certain deposit for a future investment. The higher this deposit is, the more probable it is for the staker to be chosen in order to validate new transactions and create new blocks. When the network is required to add new blocks to the blockchain, it will randomly select one of these stakers, based on how high their stake is. Ethereum 2.0 for example is currently using the PoS system. Figure 4 depicts how Proof of Stake works.

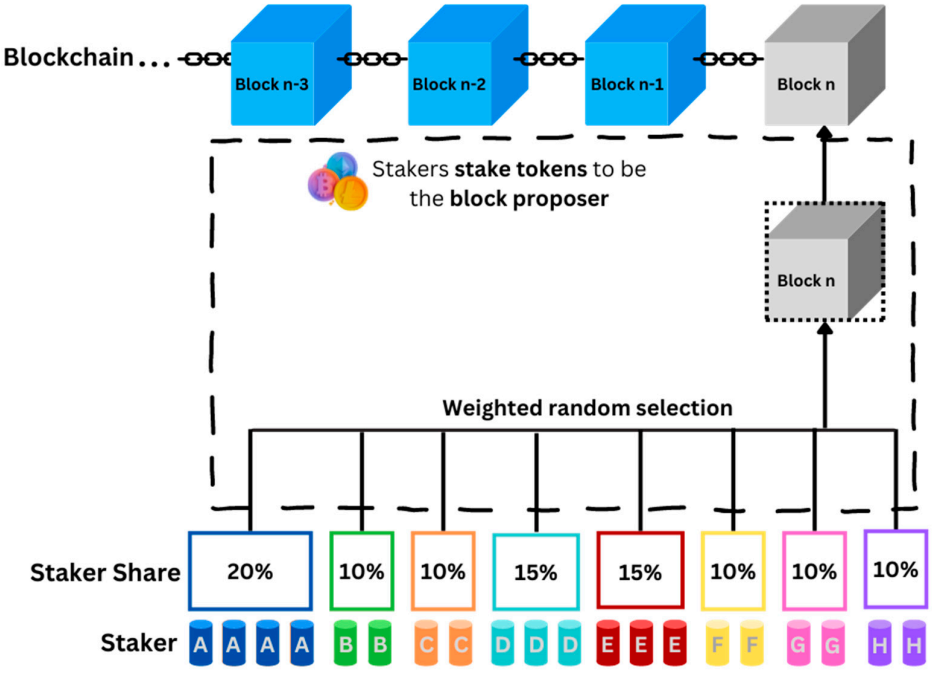

Figure 4. Proof of Stake (PoS).

 doi:10.20944/preprints202407.1977.v1

2.2.1.3. Delegated Proof of Stake (DPoS)

The Delegated Proof of Stake algorithm is an evolution of the traditional Proof of Stake described previously. In this consensus algorithm, a distributed voting system is promoted, in which members vote a limited number of witnesses, or delegates, to secure the network, make sure no acts of fraud are being committed, validate transactions and create new blocks. This algorithm is based on a reputation system where dishonest delegates can be voted out of the system. In DPoS, the number of delegates is kept to a minimum in order to be able to achieve improved efficiency, scalability and low energy consumption. The DPoS algorithm aims to create a more scalable form of consensus which will be able to significantly increase transaction speeds and reduce costs. This makes DPoS a rather suitable system for distributed applications requiring high transaction propagation rate. Figure 5 shows in detail how Delegated Proof of Stake works.

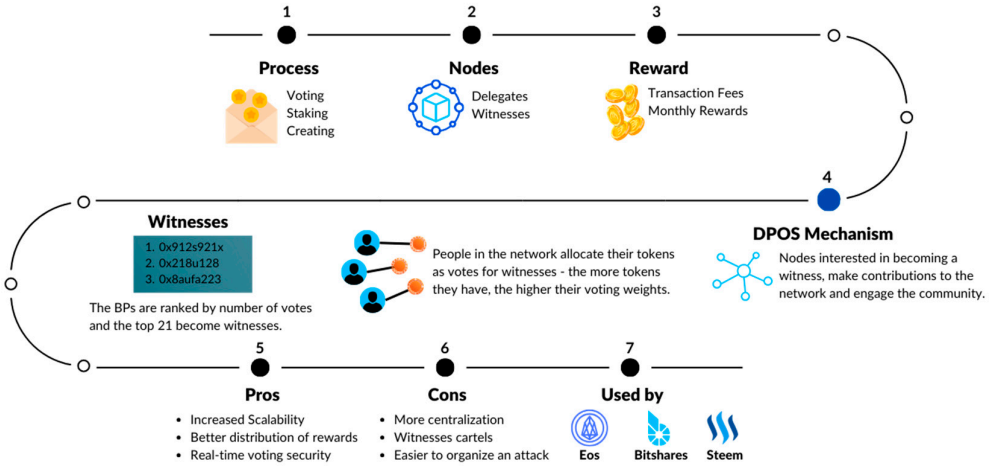

Figure 5. Delegated Proof of Stake (DPoS).

2.2.1.4. Practical Byzantine Fault Tolerance (PBFT)

Practical Byzantine Fault Tolerance algorithms are highly relevant to distributed systems as they address the Byzantine Generals' Problem. To put it briefly, the issue involves a group of Byzantine generals (or nodes in the case of a blockchain) reaching a consensus on a collective course of action. The Byzantine generals then engage in combined action by coordinating several army units to attack a citadel simultaneously. Regarding blockchains, this involves obtaining consensus on whether to verify a block or set of transactions. The difficulty lies in the fact that messages sent between the generals must traverse enemy territory and might potentially be lost without alerting the sender or the receiver, akin to traveling via an unstable, decentralized network. Additionally, some of the generals might be traitors who want to disrupt the combat strategy by transmitting misleading or altered communications, or by ignoring messages altogether. The problem is to guarantee that faithful generals can come to an agreement on the offensive strategy, without a few disloyal individuals leading them to choose an ineffective plan. In blockchain terminology, a limited number of untrustworthy or possibly malicious nodes should not have the ability to influence the confirmation of a fraudulent block or set of transactions. These transactions are verified individually by well-known and trusted validators, making these algorithms more suitable for implementation in trusted environments. Figure 6 depicts the way Practical Byzantine Fault Tolerance works.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 25 July 2024 doi:10.20944/preprints202407.1977.v1

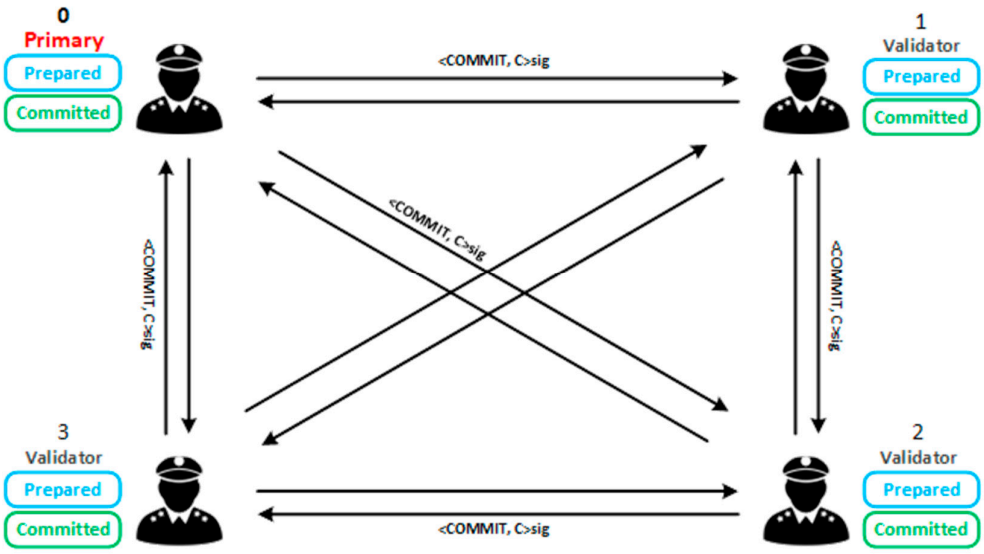

Figure 6. Practical Byzantine Fault Tolerance (PBFT).

2.2.1.5. Proof of Authority (PoA)

Proof of Authority is another consensus algorithm used in blockchain networks. In this system, approved accounts act as validators and are the ones responsible for validating blocks and transactions. PoA algorithms are based on the reputation and the identity of its validators. They are chosen based on their reliability and overall commitment to the network. Usually, the identity of these validators is public and easily verifiable, thus adding an extra layer of accountability to the whole PoA system. Since those validators put their identity and reputation at stake, they are quite motivated into maintaining and enhancing the integrity of the network. Generally, PoA's processes of transaction validation are much faster than PoW's or PoS's, since validators are limited and well-known in this mechanism, making it ideal for organizations requiring more scalable blockchain solutions. Figure 7 shows us how Proof of Authority really works.

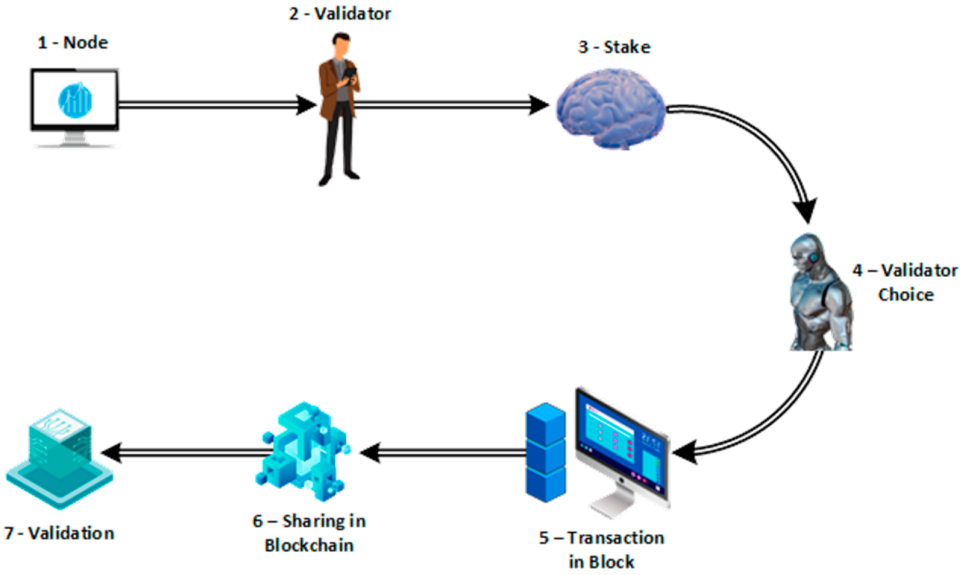

Figure 7. Proof of Authority (PoA).

 doi:10.20944/preprints202407.1977.v1

Table 1. Comparison of Blockchain consensus mechanisms.

Consensus Mechanism	Energy Consumption	Security	Scalability	Use Cases
Proof of Work (PoW)	High	High, but energy-intensive and vulnerable to 51% attacks	Limited by transaction throughput (e.g., Bitcoin ~7 transactions per second)	Bitcoin, Ethereum (transitioning away), Litecoin
Proof of Stake (PoS)	Low to Moderate	High, dependent on the amount of staked tokens	Better than PoW, but still faces challenges with network congestion	Ethereum 2.0, Cardano, Tezos
Delegated Proof of Stake (DPoS)	Low	High, but relies on a smaller number of validators	High scalability due to fewer validators needed for consensus	EOS, Tron, Steem
Byzantine Fault Tolerance (BFT)	Moderate	Very high, resilient to up to 1/3 of nodes failing or acting maliciously	High scalability with fast transaction finality	Hyperledger Fabric, Tendermint (used in Cosmos)
Proof of Authority (PoA)	Low	High, but depends on the trustworthiness of authorities	High scalability with quick consensus due to limited validators	VeChain, POA Network, Private blockchains

3. Distributed Systems: Concepts and Challenges

Distributed systems are interconnected networks of independent terminals that work together seamlessly in order to perform various tasks. These systems distribute the tasks they have to complete across multiple platforms, that communicate with each other and coordinate their actions through exchanging messages amongst themselves. Unlike centralized systems, in which a single terminal has to process all the tasks, distributed systems become more reliable and scalable by incorporating this kind of task-sharing architecture.

In today's advanced computing landscape, where data storage and processing power demands have skyrocketed, the use of distributed systems has become an absolute necessity and of immense value. They have become the very foundation on which all modern systems have been built, from cloud computing services and IoT devices to online banking systems and social media platforms. These systems have the ability to handle and process unprecedented amounts of data while responding simultaneously to millions of requests from users all around the world, at any given time.

3.1. Core Concepts of Distributed Systems

Nodes and networks: as we mentioned previously, distributed systems are networks comprised of independent computers. These computers, that work together in order to complete a set of tasks, are also known as nodes. These nodes exchange messages in order to effectively communicate with

 doi:10.20944/preprints202407.1977.v1

each other. Each of these nodes is its own set of a complete terminal (both hardware and software) and there are variations in what their roles are in the network, their resources and their capabilities. Such diversity noted among these nodes is what empowers distributed systems to effectively leverage their vast resources and capabilities, thus enhancing their efficiency and flexibility even further. The architecture of these systems is being widely used in creating both local area networks (LANs) and wide area networks (WANs).

Decentralization: in centralized systems, there is one main unit or a mainframe which controls how the entire network will operate and undertake tasks. If the mainframe crashes, the entire system crashes along with it. In decentralized systems, there is not one single mainframe that controls everything. Instead, control is spread out to the entire network's terminals, or nodes, each one of them working independently. Thus, in case of a node's breakdown, the rest of the system keeps functioning well and can complete tasks.

Distributed systems have been utilizing decentralized cooperative algorithms for the purposes of achieving better fault-tolerance rates, higher performance and better load balancing. Since decentralized environments have emerged, such as peer-to-peer networks, decentralized algorithms have become a necessity in order for these networks to be able to coordinate tasks, communicate effectively and make the right decisions locally. There are three well-established cooperative algorithms which are being discussed below [7].

- Voting is a cooperative algorithm used by decentralized systems in order to make decisions collectively. In such a network, each node will place its vote on certain decisions like which version of a specific set of data is correct. The nodes (or computers) will communicate their "votes" with each other, based on a set of rules that each one has, subsequently making a decision based on the total number of votes the corresponding option gathered [7].
- Token Ring is another cooperative algorithm tasked with managing the network's communication system. In this kind of network, all nodes are connected with each other in the shape of a ring. Within this ring of nodes, there is a digital token which moves around the network, to the node that wants to send a message. Without this token, a node cannot communicate with the other nodes in the network. Once a node has sent its message, it passes the token on to the next node in line to communicate [7].
- Market-based is the third cooperative algorithm of the list that is being employed in a decentralized distributed system. This algorithm works like a "trading marketplace"; nodes offer specific resources and ask for something else in return. For example, a node may offer processing power to another node in exchange for some storage space. These algorithms help a network allocate its resources in the most efficient way, taking into consideration each node's demands and maximizing the network's overall performance.

Scalability: the concept of scalability refers to a system's capability to handle any extra load of work given to it or its potential to accommodate it. Scalability has two important parameters; size and location. Size scalability is about the number of nodes (computers or servers) added into the network and how well this network can handle more nodes or tasks given to it, without it having any negative repercussions to its performance [8]. When it comes to location, geographical scalability is about a system's ability to maintain its robustness and effectiveness across larger geographical areas. Think of it as an efficient delivery service that can reach its customers fast, no matter how spread out they are.

An illustrative case is Twitter's transition from a monolithic architecture to a microservices-based distributed system. Initially, Twitter faced significant scalability issues, with frequent downtimes during peak usage. By migrating to a distributed system with microservices, Twitter improved its scalability, allowing it to handle millions of users simultaneously. This transition, however, required overcoming challenges related to service orchestration, data consistency, and fault tolerance.

Transparency: distributed systems have the ability to appear to its users and developers as one single unit (network) rather than many autonomous systems working together. The users should not be aware of what is the location of these systems or what files are being transferred. Below, the 7 different types of transparencies are presented [9].

 doi:10.20944/preprints202407.1977.v1

Table 2. 7 types of Transparencies.

Type	Description
Access	This kind of transparency hides from the end-user the data behind the system or the way this data is accessed. A prime example of this is ATMs. We do not see how they work but they do their job and we get our money.
Location	The location transparency hides from the user where a system's resources (or services or files) are located but it can be accessed as if it were a user's local system.
Concurrency	This type of transparency allows for multiple users to access resources all at the same time, without any of them interfering in the others' work. One example of this transparency is the way colleagues can work on the same text document simultaneously, in real time.
Replication	Replication transparency makes sure to hide the replicated resources and data from the user and only show them one instance of the data they require.
Failure	This transparency hides from the user a system's failure and recovery of its components. Every time a server crashes, a user's request is automatically rerouted and executed by another server, without the user ever realizing the crash.
Migration	Migration transparency allows a system to transfer its resources and processes within the system, without the user ever noticing or being affected by it.
Performance	The system has the ability to reconfigure itself in order to improve its performance, again without the end-user ever noticing or being affected by this process.

3.2. Challenges in Distributed Systems

Distributed systems may offer some very important features but they are not without their challenges because of their complexity and their constant need for coordination across multiple platforms and locations. Some key challenges distributed systems face are presented below.

Fault tolerance: Distributed systems, much like any other system, are prone to hardware or software faults. The way a distributed system responds and is capable of resolving these faults is known as fault tolerance. Fault tolerance as a concept is based on two components; failure detection and recovery. Generally, there are two main approaches in coping with fault tolerance; proactive and reactive fault tolerance [10].

Proactive fault tolerance: the main idea here is to be able to predict when faults will occur and what kind, and to take all the necessary actions required in order to address them properly when the time comes. Here, there are 3 techniques that are mostly used:

Table 3. 3 techniques of Proactive Fault Tolerance.

Type	Description
Preventive maintenance	This technique involves the regular maintenance of the entire system and all of its components in order to keep it robust and prevent its failure.
Predictive analysis	This technique is about analyzing patterns and behaviors of a system, as well as its overall performance, in order to identify potential issues that could cause system failure and address them properly. It works much like the process of weather forecasting.

 doi:10.20944/preprints202407.1977.v1

Rejuvenation	This technique involves the frequent rebooting of a system, or parts of it, in order to clear any errors or bugs that may have accumulated in the system over a period of time.

Reactive fault tolerance: this type of techniques is used after a failure has already occurred in a system and tries to mitigate as much of the damage done as possible. The techniques being employed most frequently here are:

Table 4. 4 techniques of Reactive Fault Tolerance.

Type	Description
Redundancy	This technique involves adding extra hardware or software that are not necessary for a system to work properly, but can be utilized in case of a failure, in order to provide a fallback solution. You can think of it as having a spare tyre in the car's trunk, in case of a tyre burst.
Replication	This method involves the duplication of important data or components across different parts of a system so that every time a failure occurs, a copy can be deployed without interrupting the system's main functions.
Checkpoints and Rollbacks	This technique works much like an operating system's restore point feature; it saves a state of the system at certain points (known as checkpoints) that works well and, when a failure happens, the system will roll back to its last saved point, thus restarting its function from that specific checkpoint.
Failover	This last technique is about having an entire backup system that will start working automatically once the main system faces a failure or crashes entirely. The process has to happen so quickly that the user won't notice any difference in the way the system works. Think of it as a backup power generator that starts working automatically once the main power system of a building goes out.

A well-known example of fault tolerance challenges is the 2012 AWS (Amazon Web Services) outage. A simple configuration error in one of AWS's Elastic Load Balancers led to a series of failures, affecting many popular services, including Netflix and Reddit. This incident highlighted the complexity of achieving fault tolerance in large-scale distributed systems and the need for robust mechanisms to handle failures gracefully [11].

Consistency: consistency in a distributed system is about the capability of the entire system (and all of its components) to present the same data, at the same time. This is very important for the system, as it makes it look reliable and robust. Maintaining this level of consistency, though, has proved to be a challenge for all distributed systems.

First of all, the different types of hardware or software platforms a distributed system is comprised of is quite a challenge to address on its own. Different nodes may have different basic capabilities and features such as storage capacity, processing speed and data management protocols, something that could prove to be a problem when it comes to the uniformity of data updates [12].

Secondly, the way nodes are placed in a network geographically can play a significant role in the overall network's latency. This latency could lead to potential data dissemination and communication delays. Simply put, when data is updated in a node, there could be a significant delay before other nodes in the network are updated with the same data, therefore leading to conflicting information being presented to different users. This, in turn, undermines the network's integrity immensely [13]. For example, Google Spanner, a globally distributed database, addresses latency issues by using synchronized clocks and advanced algorithms to ensure low-latency and high-consistency transactions. However, this solution comes with the complexity of maintaining precise

 doi:10.20944/preprints202407.1977.v1

time synchronization across data centers worldwide, showcasing the trade-offs involved in managing latency in distributed systems. Figure 8 depicts Google Spanner's architecture.

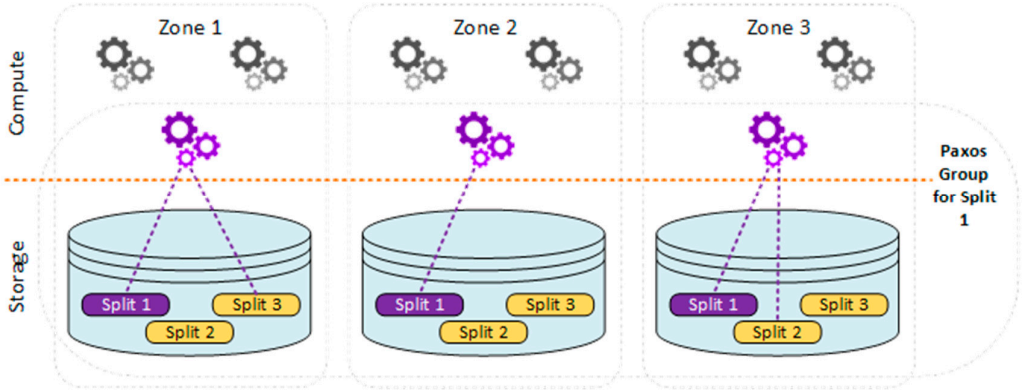

Figure 8. Google Spanner architecture.

Last but not least, in distributed systems, multiple processes usually occur across a number of nodes, all at the same time, and this brings forth a need for concurrency control. Concurrency control, however, has proved to be quite challenging. Being able to manage concurrent actions in a distributed system, without causing data conflicts or other discrepancies in the network, requires the use of highly sophisticated synchronization mechanisms. Implementing those mechanisms, however, could prove a challenging task as well, due to trade-offs needed between the three characteristics (consistency, availability, partition tolerance) featured in CAP (Brewer's) theorem [14].

A few consistency models have been proposed so far, that could address the challenges mentioned previously. The most common ones are strict consistency and eventual consistency. Strict consistency may offer an especially high level of uniformity but this often affects the availability and performance of a system. Eventual consistency, on the other hand, offers performance boosts and greater flexibility but it also introduces temporary inaccuracies.

A real-world example of consistency issues is the "split-brain" problem in Apache Cassandra, a popular distributed NoSQL database. In a split-brain scenario, network partitions can lead to multiple nodes accepting writes independently, resulting in data inconsistencies. Resolving these inconsistencies requires complex conflict resolution mechanisms and can lead to potential data loss or corruption. Figure 9 shows a multiple data center cluster with 3 replica nodes [15].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 25 July 2024 doi:10.20944/preprints202407.1977.v1

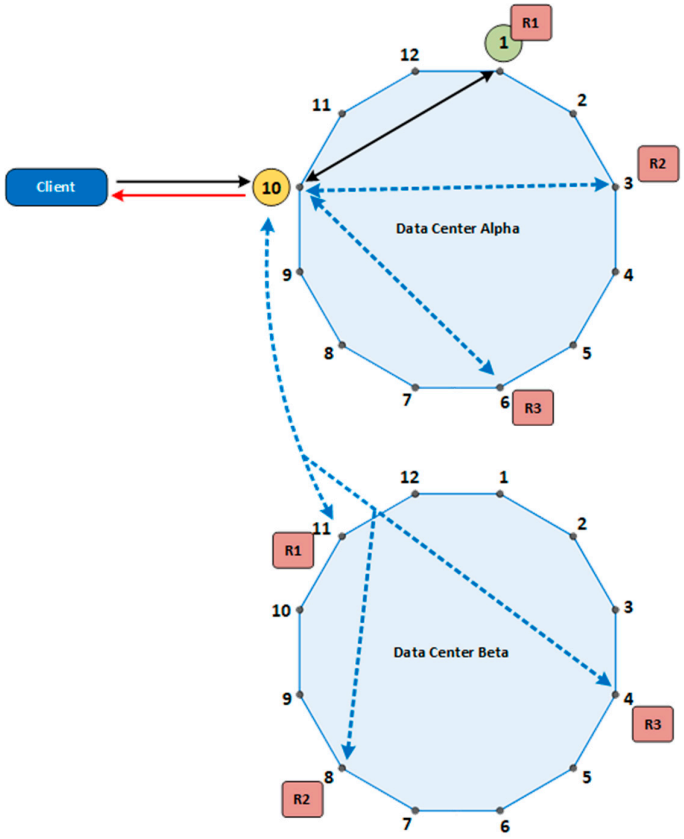

Figure 9. Multiple data center cluster with 3 replica nodes and consistency set to LOCAL_ONE.

Partition tolerance: partition tolerance has to do with a distributed system's ability to keep operating even if partitions keep occurring in the network that result in nodes, or groups of nodes, being unable to communicate effectively with each other. Hardware malfunctions, network failures or other kind of disruptions are the causes of such partitions [16]. Therefore, being able to ensure that a network remains partition tolerant will greatly impact its reliability and availability.

The real challenge of maintaining high levels of partition tolerance lies in keeping a balance between other characteristics as well, such as consistency and availability. In a distributed system, however, only two of the three characteristics (consistency, availability, partition tolerance) can be achieved, as stated in the CAP theorem.

The CAP theorem, also known as Brewer's theorem, is a fundamental principle in the design of distributed systems [17]. Formulated by Eric Brewer in 2000, it states that it is impossible for a distributed data store to simultaneously provide all three of the following guarantees:

1. Consistency (C): Every read from the system receives the most recent write or an error. In other words, all nodes see the same data at the same time.
2. Availability (A): Every request (read or write) receives a non-error response, without the guarantee that it contains the most recent write.
3. Partition Tolerance (P): The system continues to operate despite network partitions, where communication between some subsets of nodes is lost.

According to the CAP theorem, a distributed system can satisfy at most two of these three guarantees simultaneously:

- CA (Consistency and Availability): These systems reject partitions, meaning they require a consistent network. If a partition occurs, the system must either sacrifice consistency or availability.
- CP (Consistency and Partition Tolerance): These systems remain consistent in the presence of network partitions but may not be available to all nodes.

 doi:10.20944/preprints202407.1977.v1

- AP (Availability and Partition Tolerance): These systems remain available even when network partitions occur but may not guarantee consistency.

Figure 10 summarizes the CAP theorem's key points.

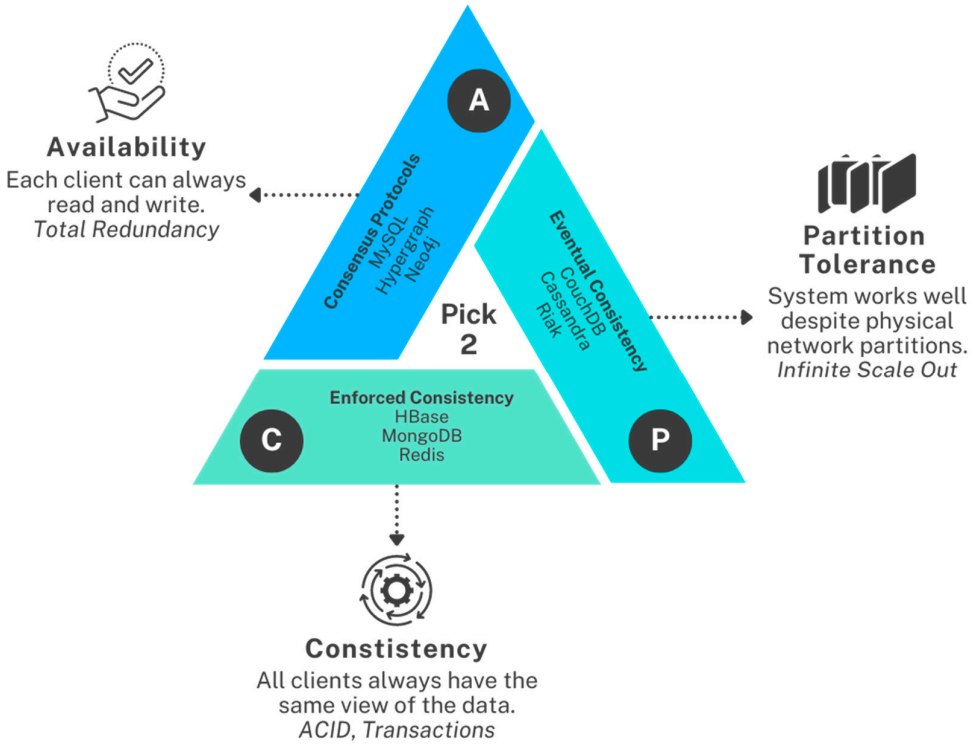

Figure 10. CAP theorem.

In practical terms, no distributed system can achieve perfect consistency, availability, and partition tolerance simultaneously [18]. Therefore, systems' designers have to make decisions about the necessary trade-offs between these three characteristics and the expected network requirements needed and overall environment. For instance:

- Databases like Cassandra and DynamoDB: Prioritize availability and partition tolerance (AP), allowing them to remain available during network partitions but possibly returning stale data.
- Systems like HBase and MongoDB: Often focus on consistency and partition tolerance (CP), ensuring data consistency across partitions at the cost of potential availability issues during network failures.
- Relational databases with distributed architectures: Tend to focus on consistency and availability (CA), often at the expense of partition tolerance, requiring a reliable network to function correctly.

Security: security is one of the most vital challenges distributed systems have to address in the most effective way. When talking about security, making sure the users' privacy and data's integrity are both well protected is of the utmost importance. One way of ensuring those is the system's authentication mechanisms [19]. These mechanisms need to be robust and constantly up-to-date, in order to be able to repel attempts for unauthorized access while making sure legitimate users can have access to the resources they need.

The second challenge that arises, regarding security, has to do with authorization and control access. The systems need to be able to determine what is the right access level for each individual user. That's why different policies need to be defined and enforced, so that the system knows who has access to what and under what conditions. While authorization mechanisms are essential to be imposed in a system, implementing methods that ensure data's confidentiality and integrity is equally important. This could be achieved, first and foremost, by establishing encryption techniques

 doi:10.20944/preprints202407.1977.v1

in the network, for both data at rest and in transit [20]. Furthermore, care should be taken into the implementation of detection and mitigation mechanisms for data tampering.

Lastly, one more challenging aspect of security is the implementation of non-repudiation and auditability mechanisms in a distributed system. Non-repudiation is needed so that the participants of a transaction cannot question or outright deny their participation in it, while auditability is responsible for tracking and examining a system's activities. These two mechanisms are quite difficult to be implemented due to the need for total synchronization and secure logs across multiple locations.

A notable example is the 2017 Equifax data breach, where attackers exploited a vulnerability in a distributed web application framework to access sensitive data of over 140 million consumers. This incident underscores the importance of robust security measures, including regular patching, intrusion detection systems, and secure communication protocols in distributed systems [21].

4. The Intersection of Blockchain and Distributed Systems

When we integrate distributed systems with blockchain decentralized ledger technology, we are talking about an immensely significant technological advancement in the world of computer networking, which addresses challenges regarding decentralization security and trust, and offers novel perspectives and solutions [22]. Blockchain is well-known for its three main features of transparency, immutability and security, and it is these attributes that have made so many industries, like healthcare and the financial sector, to incorporate it in its main functions [23]. Distributed systems, on the other hand, were designed in order to facilitate resource sharing, provide a certain level or scalability and improve overall performance. However, they also faced challenges such as fault tolerance, data consistency and resource management.

Incorporating blockchain technology into distributed systems offers various synergistic benefits. To start, this intersection addresses trust problems among decentralized nodes in a network, thus enhancing its overall integrity and security. The ledger acts as an indisputable source of trust, making sure data is consistent across all nodes in the system [24]. Additionally, the transparency feature blockchain offers is in complete alignment with a distributed system's nature, which then allows for the equitable sharing of resources and promotes collaboration among participants.

Furthermore, blockchain utilizes the consensus mechanisms that were mentioned previously (e.g. Proof of Work and Proof of Stake). These mechanisms introduce a democratic procedure in transaction verification and the maintenance of the ledger, thus granting the distributed nodes the ability to achieve consensus regarding the state of the system. Consensus is a vital mechanism in distributed systems, especially when malicious or faulty nodes are present in a network, since it renders a system available and reliable [25].

In addition, blockchain's peer-to-peer (P2P) nature works in perfect sync with distributed systems, since they both operate on networks in which nodes communicate directly and collaborate effectively with one another. This peer-to-peer feature also helps the network decentralize even further, as it enables nodes to function more autonomously, sharing data and resources with each other without the constant need for intermediaries [26]. Figure 11 shows how a decentralized distributed system works while integrating Blockchain's peer-to-peer features.

 doi:10.20944/preprints202407.1977.v1

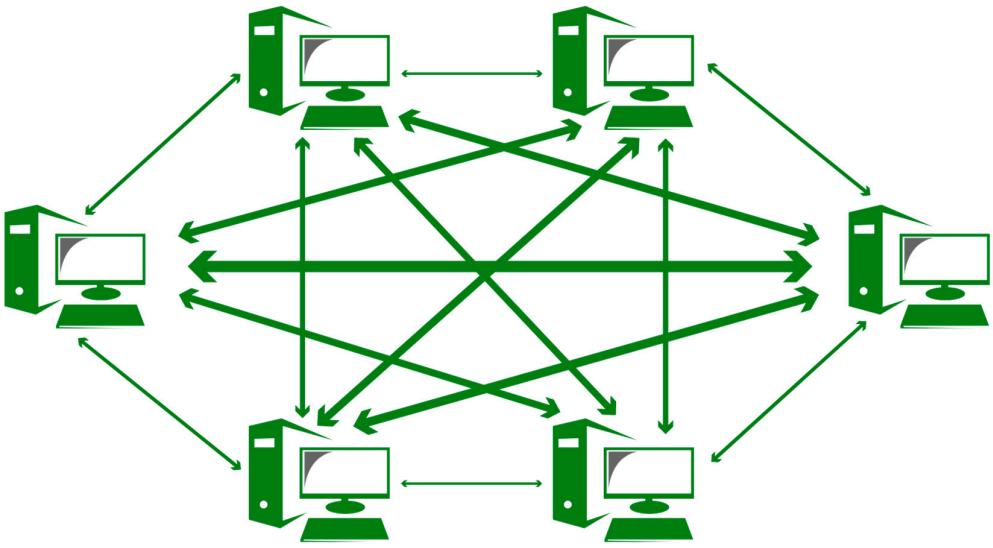

Figure 11. Decentralized systems integrating Blockchain's P2P features.

When it comes to data integrity, In traditional distributed systems, data integrity relies heavily on centralized databases and trusted third parties. This centralization can lead to single points of failure and increases the risk of data tampering or corruption. For instance, if the central database is compromised, all connected nodes might be affected, leading to widespread data integrity issues. Blockchain technology enhances data integrity through its immutable ledger. Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring that all nodes in the network have access to the same, unaltered data. This feature is particularly beneficial in environments where data integrity is critical, such as financial transactions or healthcare records. The decentralized nature of blockchain removes the reliance on a single point of control, reducing the risk of data tampering [27].

When it comes to the matter of security, in traditional systems security relies on centralized control and access management, which can be vulnerable to attacks targeting the central authority. Data breaches and unauthorized access can compromise the entire system. Blockchain deploys advanced cryptographic techniques in order to make sure data keeps its integrity and confidentiality in a network. Cryptographic algorithms encrypt each transaction and link it to all the previous transactions, thus creating a chain. This mechanism, along with the creation of public and private keys, ensures that only authorized users can have access or modify the data. This whole procedure adds an extra layer of security in conducting transaction within a distributed system. Apart from this, blockchain technology incorporates an immutable ledger, which is very difficult to alter. This feature of immutability is enforced in the entire network by using consensus algorithms that requite total agreement among the nodes, before any change can be applied. Immutability not only enhances the overall security of the network even further, by preventing unauthorized tampering of the data, but also strengthens the integrity of the entire system.

Regarding fault tolerance, in traditional distributed systems it typically involves replication and redundancy strategies managed by central controllers. However, these strategies can still be vulnerable to systemic failures and may not be entirely effective in preventing data loss during network partitions. Blockchain enhances fault tolerance through its decentralized architecture. Each node in a blockchain network maintains a complete copy of the ledger, allowing the system to continue operating even if several nodes fail. Consensus mechanisms ensure that the network can reach agreement on the state of the ledger despite individual node failures, providing robust fault tolerance [28].

Scalability in traditional distributed systems can be challenging, as increasing the number of nodes often leads to greater complexity and higher costs. Centralized databases can become bottlenecks, limiting the system's ability to handle large-scale operations. While blockchain offers

 doi:10.20944/preprints202407.1977.v1

many advantages, scalability remains a challenge. However, emerging solutions such as sharding, off-chain transactions, and layer-two protocols like Lightning Network are being developed to enhance blockchain scalability. These innovations aim to allow blockchain networks to handle more transactions per second, making them more suitable for large-scale applications [29].

Lastly, transparency in traditional systems is often limited, with data access restricted to certain entities. This can lead to trust issues among stakeholders, as they must rely on the central authority to provide accurate and complete information. Blockchain offers a public ledger, which is usually accessible to everyone in the network and provides transparency in every transaction and data change. This prevents secrecy in actions taken within the network and all users within it can audit and verify each transaction independently. Furthermore, as mentioned previously, blockchain records every single transaction with a digital timestamp and links it to all previous transactions [30]. This provides a level of traceability to the data and its history, something that can be particularly useful in industries like supply chain, in which it is important to be able to verify the authenticity and history of products. Another mechanism that adds to blockchain's transparency feature is a smart contract. Blockchain utilizes smart contracts, which are essentially self-executing pieces of code, directly containing the terms of an agreement. They are used in order to automate and enforce contractual obligations and without the use of intermediaries, enhancing the transaparency of agreements and transactions within a system even further. Table 5 summarizes the differences between a traditional centralized system and a blockchain-integrated system.

Table 5. Comparison of traditional systems vs. blockchain-integrated systems.

Dimension	Traditional Systems	Blockchain-Integrated Systems
Data Integrity	Relies on centralized databases; prone to tampering or corruption if the central authority is compromised.	Ensures data integrity with an immutable ledger; data cannot be altered once recorded, reducing the risk of tampering.
Transparency	Limited transparency; data access is often restricted and requires trust in the central authority.	High transparency; all participants can view the entire transaction history, enhancing trust and accountability.
Fault Tolerance	Managed through central controllers with replication and redundancy strategies; still vulnerable to systemic failures.	Decentralized architecture enhances fault tolerance; each node maintains a complete copy of the ledger, ensuring continuity despite individual node failures.
Scalability	Centralized databases can become bottlenecks; scaling up often increases complexity and cost.	Scalability remains challenging, but emerging solutions like sharding and layer-two protocols (e.g., Lightning Network) are improving transaction throughput.
Security	Centralized control is vulnerable to attacks targeting the central authority, leading to potential data breaches.	Enhanced security through cryptographic techniques and decentralized consensus; eliminates single points of failure, making the system more resilient to attacks.

5. Decentralized Decision-Making

Understanding the decentralized decision-making mechanisms is pivotal when developing distributed technologies, especially where leveraging blockchain technology and related innovations is required. Traditional decision-making used to be centralized in one single authority. Decentralized decision-making, on the other hand, is the process of making decisions collectively, by multiple

 doi:10.20944/preprints202407.1977.v1

individuals and across different locations or organizational levels. In the context of decentralized distributed systems, multiple nodes make the necessary decisions instead of one mainframe (or server), thus enhancing these systems' efficiency, resilience and democratic governance [31].

5.1. Key Principles of Decentralized Decision-Making

One of the most important principles of decentralized decision-making, at a foundational level, is consensus. It is the process of agreeing on a set course of action or a single version of the truth by all the nodes in a decentralized system. Consensus is vital for a system to maintain its integrity and consistency, since it ensures that all participants accept and recognize the decisions being made in the network, such as the validation of a transaction. Consensus uses several mechanisms (e.g. PoW, PoS, etc.) in order to help the system reach an agreement, combining efficiency with fairness and inclusivity [32].

A second key principle included in decentralized decision-making is autonomy. Autonomy refers to the capability of an individual node or agent to operate and make decisions entirely on its own, within the network, without a centralized authority mechanism deciding for it. This autonomy feature makes sure a decentralized system can continue to work properly even if certain nodes selectively start malfunctioning or stop functioning altogether, thus strengthening the system's resilience and fault tolerance [33].

The third key principle of decentralized decision-making is trustlessness. Trustlessness means that a system operates in such a manner that no trust is required by the parties involved. This is also an integral feature of blockchain technology. The participants of a network can interact with each other in a secure way because they know that the system will enforce security rules and validate transactions impartially, using consensus algorithms and cryptographic verification. This feature makes the use of intermediaries obsolete and reduces vulnerabilities caused by relying on third parties [34].

Combining all three of these principles makes a decentralized system more robust, democratic and transparent. The system can upscale its operations effectively while maintaining its strong security and enabling P2P interactions. Such systems are of immense value to industries like financial and healthcare services, supply chain and more. Figure 12 shows the 3 main principles around decentralized decision-making.

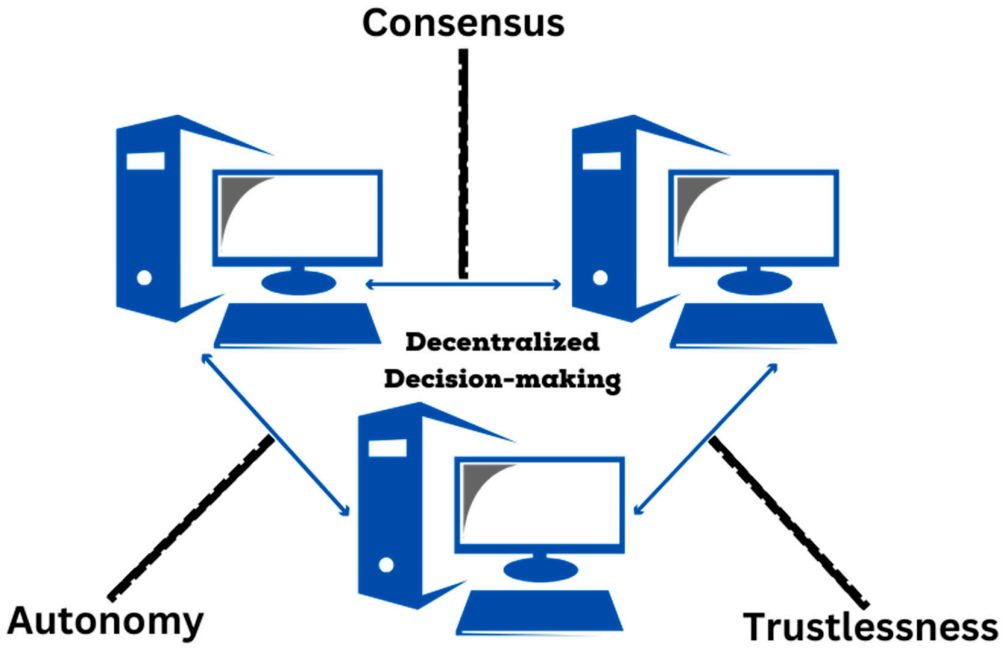

Figure 12. Key principles of decentralized decision-making.

 doi:10.20944/preprints202407.1977.v1

5.2. Game Theory and Decentralized Decision-Making

Game theory is a mathematical framework which was developed in order to comprehend interactive decision-making operations among rational agents, and this can be especially applied in decentralized decision-making in distributed systems. What makes game theory relevant to decentralized decision-making is its ability to model and predict node behaviors, in a system where no single authority dictates the participants' actions. As highlighted previously, nodes in a decentralized network must make decisions that keep a balance between personal incentives and the collective good of that network. This is where game theory comes in, helping in comprehending these dynamics by examining various scenarios, or "games", that showcase how rational nodes are likely to behave under different kinds of scenarios. Some prominent examples of these scenarios are the Nash Equilibrium and the Prisoner's Dilemma [35].

In blockchain technologies, the use of game theory is fundamental when designing consensus algorithms that strengthen the network's security and promote the participants' cooperation. A prime example of how game theory contributes to blockchain is Bitcoin's Proof of Work system. Here, game theory explains why it is much more beneficial for rational miners to follow protocol rules; it is because not following the typical consensus rules of a blockchain system is much less profitable for them than honest contributing (through the process of mining). Additionally, game theory demonstrates how trust can be achieved through mechanisms and incentives that promote cooperation between the participants as the most logical path. Thus, game theory highlights the concept of trustlessness in decentralized distributed systems [36].

5.3. Decentralized Decision-Making Mechanisms

Consensus Mechanisms

Blockchain networks' ability to let participants achieve a collective agreement on the state of the blockchain in a distributed and trustless manner helps to explain its functioning in great part through consensus processes.

Consensus method known as Proof of Work (PoW) is one wherein miners compete to solve complex mathematical challenges. This mechanism authenticates transactions and adds new blocks to the blockchain. This method uses significant computer resources—also known as hashing—to find a hash value less than a designated target. The first miner who solves the challenge sends the response to the network. Should additional nodes validate the answer, the newly created block is included to the blockchain. PoW is vulnerable to criticism despite its great security and durability due to its high energy consumption and scaling restrictions [37].

Another well-known consensus system addressing some of PoW's shortcomings is Proof of Stake (PoS). Block validators in PoS are chosen depending on their bitcoin count and willingness to "stake," or lock down, as collateral. Based on their network connectivity, validators are selected to build fresh blocks and validate transactions. PoS hopes to lower energy use and increase scalability by measuring participation using stake instead of compute capability. Because they run the danger of losing their staked tokens should they approve false transactions, validators are financially motivated to operate honestly [38].

A variation of PoS, delegated proof of stake (DPoS) improves scalability and efficiency even further. Token holders in DPoS can cast restricted number of delegates or block producers to represent them in block generation and validation. Selected based on criteria like reputation, technical knowledge, and network contributions, delegates create blocks in a round-robin style one at turn. Token holders' voting weight influences how much delegates affect block generation. By means of token-holder voting, DPoS seeks to preserve decentralization while lowering the validator count, hence optimizing scalability and efficiency [39].

Every one of these consensus systems has benefits and drawbacks; their fit will rely on elements like security demands, aims of decentralization, and scalability requirements. Comprehending how blockchain networks reach consensus and maintain the integrity of the distributed ledger depends on an awareness of the subtleties of these consensus algorithms.

Voting Systems

 doi:10.20944/preprints202407.1977.v1

Blockchain technology provides novel solutions for decentralized decision-making via voting systems, allowing stakeholders to engage in governance processes with transparency and security. Traditional voting methods frequently encounter difficulties such as fraudulent activities, manipulation, and a dearth of openness. Blockchain-based voting techniques resolve these concerns by offering unchangeable and easily visible records of votes, guaranteeing confidence and integrity in the decision-making procedure. Within a voting system that operates on a blockchain, anyone with a vested interest can submit their votes about proposals or modifications to the network protocol by utilizing their cryptographic keys. Every vote is documented on the blockchain, establishing an unalterable and verifiable record of voting actions [40]. The decentralized structure of blockchain guarantees that no one holds authority over the voting process, hence fostering equity and inclusiveness. Figure 13 depicts how a blockchain-based voting system works.

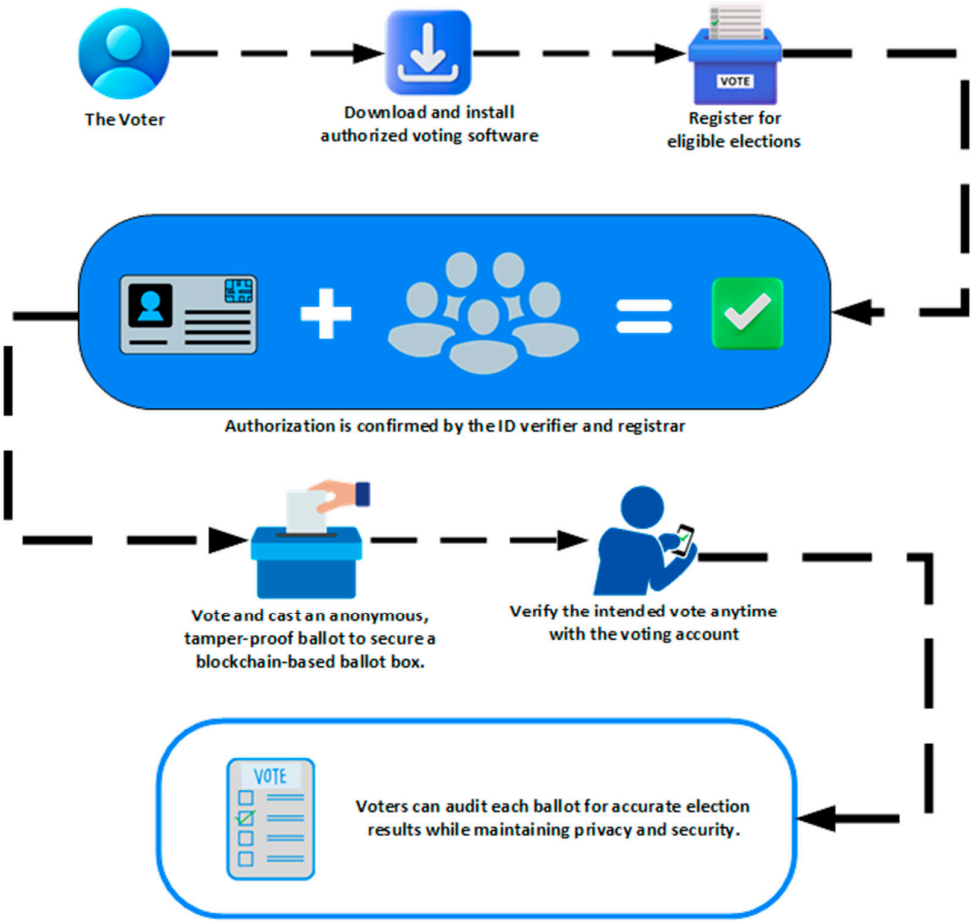

Figure 13. Blockchain-based Voting System.

Smart contracts are essential for enabling voting systems that are based on blockchain technology. Smart contracts are autonomous contracts that have predetermined rules and conditions that are inscribed on the blockchain and execute themselves. The voting process is automated through the management of duties such as voter registration, ballot casting, and result tabulation. Smart contracts provide the transparent enforcement of voting rules without the involvement of middlemen [41].

Blockchain-powered voting systems may be integrated into other forms of governance, such as decentralized autonomous organizations (DAOs) and ecosystems based on tokens. Within Decentralized Autonomous Organizations (DAOs), stakeholders exercise their voting rights to determine the allocation of cash, implement protocol updates, or make strategic determinations [42]. Token-based ecosystems employ voting methods to oversee protocol updates, parameter

 doi:10.20944/preprints202407.1977.v1

modifications, and community activities. Blockchain-based voting systems provide significant advantages in terms of openness and auditability. Given that every voting action is documented on the blockchain, stakeholders have the ability to authenticate the integrity of the voting procedure and conduct an independent examination of the outcomes. The presence of openness in this context promotes trust among those involved and strengthens the credibility of decisions made in governance. Furthermore, voting systems that utilize blockchain technology provide enhanced protection against fraudulent activities and tampering. The cryptographic properties of blockchain guarantee that votes are securely encrypted and immune to any kind of tampering once they are registered on the distributed ledger. Moreover, the decentralized structure of blockchain reduces the possibility of centralized assaults or censorship, hence strengthening the security of the voting procedure [43].

Blockchain-based voting systems still have problems like scalability, accessibility, and voter privacy regardless of its benefits. Processing vast amounts of votes on the blockchain causes computing overhead that results in scalability problems. Accessibility issues center on the requirement of users having access to cryptographic keys and internet-connected devices so they may engage in the voting process. Another crucial factor is voter privacy as blockchain-based voting systems have to strike a compromise between openness and the anonymity of particular votes [44].

Smart Contracts and DApps

A novel use of blockchain technology, smart contracts, let distributed decision-making procedures be automated. Stored on a blockchain, these self-executing contracts are designed with pre-defined rules and conditions and automatically run when those criteria are satisfied. By enabling trustless and open agreements among parties, smart contracts reduce the need for middlemen—such as attorneys or escrow services. Once implemented on the blockchain, smart contracts are one of the main characteristics that enable their execution free from human involvement. By guaranteeing objective and unbiased application of contractual requirements, this automation helps to lower the danger of conflict or fraud. Smart contracts give a great degree of dependability and assurance since their results will be carried out exactly as decided upon. This helps parties in economic transactions. Smart contracts let a lot of applications be made in many sectors. Smart contracts may be applied in finance to automate loans, insurance payouts depending on preset criteria like time triggers or external data inputs, payments, Once products are delivered and confirmed by a reputable third party, a smart contract may, for instance, immediately transfer money to a supplier.

Smart contracts have the ability to optimize several aspects of supply chain management, including product tracking, authentication, and payments. Smart contracts can increase the efficiency, risk management, and transparency of supply chain operations by utilizing blockchain technology to record each stage of the supply chain and automatically disburse payments depending on specified milestones [45].

Smart contracts have the capacity to fundamentally transform the process of drafting, executing, and enforcing contracts in the legal industry. Smart contracts enable the conversion of legal agreements into executable code, guaranteeing that contractual obligations are clear, unchangeable, and capable of being enforced. Implementing this might optimize the contract negotiating procedures, decrease legal expenses, and mitigate the potential for conflicts resulting from unclear contract wording [46].

Blockchain technology and smart contracts provide unique solutions for the management and protection of intellectual property (IP) rights. Smart contracts have the ability to automate the process of registering and transferring intellectual property rights. This ensures that the records of ownership cannot be changed and can be easily accessed by anybody. This technology streamlines the process of licensing patents, trademarks, and copyrights by automatically enforcing the terms of agreements and distributing royalties based on usage metrics recorded on the blockchain. This not only simplifies the administration of intellectual property (IP), but also decreases the likelihood of infringement and illegal use. It establishes a strong system for creators and rights holders to protect their intellectual property [47].

 doi:10.20944/preprints202407.1977.v1

Blockchain technologies and smart contracts taken together may also revolutionize the gaming industry. These technologies let players securely and honestly own and exchange digital objects, therefore enhancing the management of in-game resources. Smart contracts guarantee players may have faith in the authenticity and scarcity of their digital possessions by allowing the automation of transactions and ownership transfers for in-game products. Blockchain technology can also provide distributed gaming platforms allowing direct connection between players and producers, therefore removing reliance on centralized businesses and promoting a fairer sharing of income.

Blockchain technology and smart contracts may completely change real-estate market property transactions in the future. They provide a clear, safe, and quick system for entering property titles and enabling trading. Guaranteeing the accurate and timely implementation of all contractual obligations, smart contracts have the capacity to automate the buying, selling, and renting processes of properties. Blockchain-based property record storage helps parties to quickly confirm ownership and transaction history, therefore reducing fraud and building trust. This technology might maximize processes like mortgage approvals and property inspections, thus improving the reliability and speed of real estate transactions [48].

Furthermore, the use of smart contracts and blockchain technology may significantly enhance the healthcare industry, namely in the areas of patient data management and administrative process optimization. Smart contracts have the capability to automate the process of exchanging patient records among healthcare providers. This ensures that the transmission of sensitive information is done safely and only with the agreement of the patient. This can enhance the synchronization of healthcare delivery and alleviate administrative encumbrances. Furthermore, blockchain technology can enable the creation of transparent and unchangeable records of clinical trials, therefore improving the reliability of medical research. Smart contracts in the pharmaceutical supply chain may guarantee the genuineness of pharmaceuticals by monitoring their entire route from the manufacturer to the patient, hence minimizing the likelihood of counterfeit drugs [49].

In addition, smart contracts facilitate the functioning of decentralized autonomous organizations (DAOs), which are intricate multi-party agreements that may run independently on the blockchain. DAOs are autonomous organizations that utilize smart contracts to formalize regulations and decision-making procedures, allowing stakeholders to engage in transparent and democratic governance of the company.

While their advantages are several, smart contracts come with several possible disadvantages like possible security risks, scalability restrictions, and legal complexity. Smart contract code with security flaws can be used for exploitation, therefore resulting in either money losses or confidence breaches—both of which are likely results. Particularly for transactions that are sophisticated or very high in volume, the processing cost that smart contract execution on the blockchain imposes limits on the scalability. The main causes of the legal problems that have emerged are the lack of established legal precedents and legislative systems managing smart contracts. This so raises issues concerning their validity and obligation in the framework of court conflicts [50].

Decentralized Autonomous Organizations (DAOs)

Decentralized Autonomous Organizations (DAOs) are a groundbreaking concept within the world of blockchain technology, with the capacity to fundamentally transform corporate governance and enterprise operations. Decentralized autonomous organizations (DAOs) are entities that enable dispersed decision-making and independent performance of organizational functions. These entities function with complete transparency on the blockchain and are regulated by smart contracts. Decentralized autonomous organizations (DAOs) rely on smart contracts, which can contain organizational rules and governance systems. The members of the DAO are granted the authority to make decisions, together with their corresponding rights and responsibilities, in accordance with these smart contracts. DAOs provide openness, immutability, and trustlessness in corporate governance by dispersing these smart contracts throughout a blockchain network [51].

DAOs are characterized by their decentralized decision-making mechanism, allowing token holders to actively engage in governance processes and shape the organization's trajectory. Token holders have the ability to cast votes on various proposals, including budget allocations, protocol

 doi:10.20944/preprints202407.1977.v1

updates, and strategic choices, by utilizing their tokens as voting power. Every token symbolizes ownership in the organization, and the voting power of participants is directly equal to the number of tokens they own. Blockchain technology guarantees transparency and auditability by recording all voting activity and decision results on the blockchain, allowing stakeholders to have a clear view of the governance process. The transparency promotes confidence among members and strengthens the credibility of governance choices inside the DAO [52].

Decentralized Autonomous Organizations provide an abundance of advantages as compared to conventional centralized organizations. DAOs mitigate the potential for corruption, censorship, and single points of failure by removing middlemen and centralized decision-makers. Furthermore, DAOs facilitate worldwide involvement, granting membership and the ability to engage in organizational governance to anybody with internet access. Moreover, DAOs foster ingenuity and cooperation by offering a framework for decentralized coordination and distribution of resources. Participants have the ability to suggest ideas, establish working groups, and cooperate on projects within the DAO, which promotes a vibrant and all-encompassing environment of invention [53]. Figure 14 depicts a DAO's architecture.

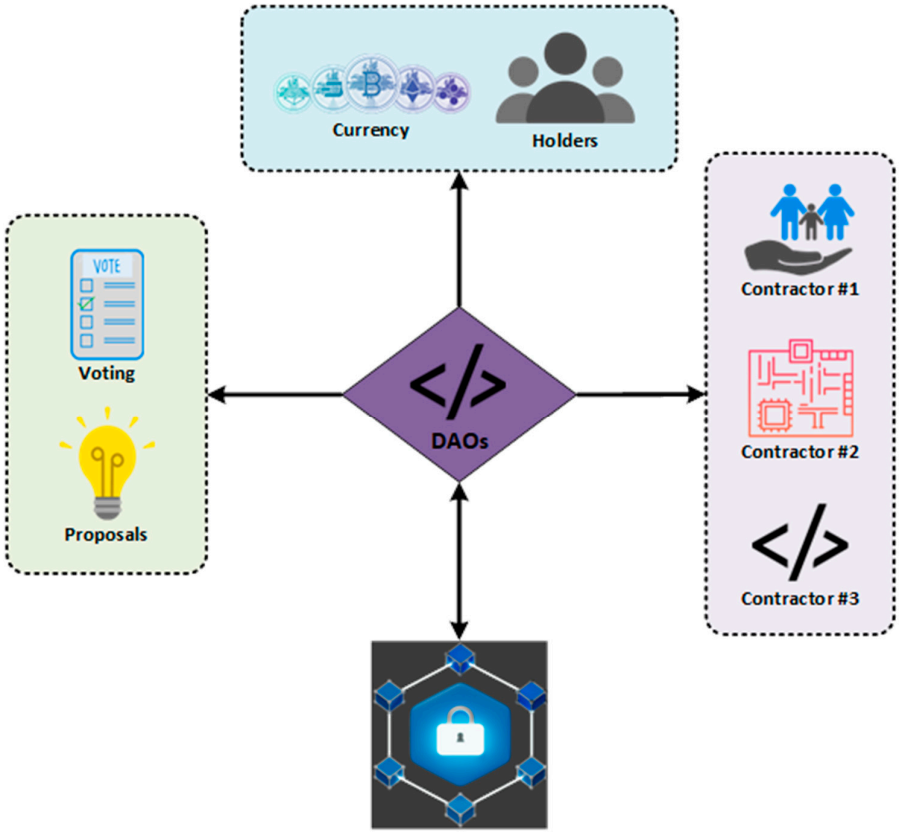

Figure 14. DAOs architecture.

DAOs, despite the numerous benefits they offer, are not without their share of difficulties and restrictions. Vulnerabilities in the security of the code of smart contracts can result in exploits or attacks that put the organization's integrity at risk. Questions regarding the legal status, liability, and enforceability of decentralized autonomous organizations (DAOs) are raised in the case of disputes or conflicts because to the legal and regulatory uncertainty that surround them.

Federated Consensus

Using cooperation among several distinct groups, federated consensus methods offer a fresh method to reach distributed consensus in blockchain networks. Unlike conventional consensus systems like Proof of Work (PoW) or Proof of Stake (PoS), in which every network member validates transactions and adds fresh blocks to the blockchain, federated consensus lets a subset of trustworthy

 doi:10.20944/preprints202407.1977.v1

entities take part in the consensus process. Fundamentally, federated consensus is a federation—a collection of pre-selected nodes or validators in charge of attaining consensus on the blockchain's state of affairs. Usually selected according to criteria including reputation, dependability, and experience, these validators work together to reach distributed consensus [54]. Comparatively to conventional consensus systems, federated consensus has two major benefits: scalability and efficiency. Federated consensus is well-suited for applications needing high speed and scalability as it may reach better transaction throughput and reduced latency by restricting the number of validators engaged in the consensus process. Furthermore, since federated consensus systems do not need for significant computing capability to evaluate transactions and network security, they can be more energy-efficient than PoW-based consensus systems. For use cases where energy consumption is a factor, including sustainable finance or environmental preservation, federated consensus especially appeals.

However, federated consensus processes encounter difficulties and compromises, regardless of their benefits. An essential obstacle is the attainment of decentralization while preserving the efficacy of the consensus process. Centralization may occur in federated consensus when the federation gets too small or if the criteria for selecting validators are not strong enough. Moreover, federated consensus techniques are vulnerable to collusion or manipulation by malevolent entities present inside the federation. Validators have the potential to conspire in order to suppress transactions, influence the consensus process, or partake in other types of nefarious activities, which can undermine the security and integrity of the blockchain network [55].

In order to reduce these concerns, federated consensus methods frequently incorporate strategies such as rotating validator roles, randomly selecting validators, and employing cryptographic techniques to guarantee fairness, transparency, and security during the consensus process. Furthermore, continuous research and development efforts are now being conducted to investigate novel methodologies and enhancements to federated consensus mechanisms, with the aim of overcoming existing limits and bolstering their resilience and decentralization.

Decentralized Governance Protocols

Protocols for decentralized governance are absolutely necessary in order to facilitate efficient decision-making in decentralized networks. They make it possible for stakeholders to propose, discuss, and vote on changes to the rules and parameters of the network before they are implemented. Regarding the administration of decentralized systems, these protocols are very necessary in order to ensure that transparency, inclusivity, and legitimacy are maintained.

The process by which modifications to the network can be suggested is a key component of the protocols that regulate decentralized governance situations [56]. Token holders, developers, and members of the community are all examples of stakeholders who have the capacity to propose modifications to the protocol, parameters, or governance structure of the network. Enhancements to protocols, revisions to parameters, modifications to funding allocations, and modifications to governance processes are all examples of topics that might be addressed in proposals. Decentralized governance protocols often give mechanisms for stakeholders to engage in debate and deliberation after a proposal has been submitted to them. This may involve the usage of communication platforms such as forums, chat rooms, or other communication channels where stakeholders are able to express their opinions, provide feedback, and take part in constructive conversation regarding the recommended modifications. Discussion periods allow for the evaluation of a variety of perspectives, the discovery of potential disadvantages and benefits, and the refinement of ideas prior to the vote process [57].

A basic element of distributed governance systems, voting systems let stakeholders vote on the acceptance or rejection of ideas together. Using their tokens or another kind of network reputation or influence, stakeholders can cast their votes. By weighting votes depending on things like token ownership, reputation ratings, or network contributions, one may make sure the decision-making process represents the interests and choices of the larger society. Depending on the particular requirements and features of the network, decentralized governance systems may apply simple majority voting, quadratic voting, or liquid democracy. Certain systems may also include

 doi:10.20944/preprints202407.1977.v1

mechanisms for delegation, wherein stakeholders may assign their voting authority to reliable agents or organizations on their behalf [58].

Important concepts in distributed governance systems include transparency and auditability, which guarantee that voting procedures and results are tamper-proof, transparent, and verifiable. The blockchain, or another distributed ledger, records all voting activity—including voter involvement, vote counting, and final results—so offering an open and unchangeable record of the decision-making process. Decentralized governance systems also seek to encourage responsibility and participation among stakeholders, hence strengthening a democratic government and community involvement. Decentralized governance systems enable people and groups to take responsibility for the networks they use and help to guide by allowing stakeholders to actively engage in decision-making processes and affect the direction of the network.

6. Applications of Blockchain in Distributed Decision-Making

The blockchain technology is used nowadays in almost every aspect of our lives and is a vital cog in the business decision-making machine. Blockchain defines all major sectors of the global economy such as finance, healthcare, supply chain and even in the government and public sector. Figure 15 summarizes the sectors in which Blockchain can impact distributed decision-making processes.

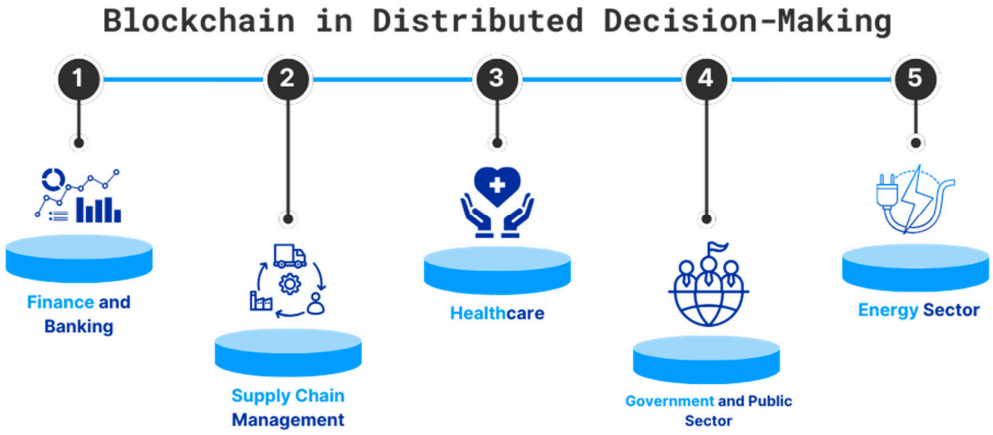

Figure 15. Sectors in which Blockchain can be applied to for distributed decision-making.

6.1. Finance and Banking

Blockchain technology is bringing about a substantial change in the field of finance and banking, particularly in the areas of transparency audits, risk assessment, and compliance management. The transformational capacity of blockchain arises from its intrinsic attributes, namely immutability, transparency, and decentralization, which are well-suited to address the crucial requirements of financial systems for precision, integrity, and protection [59].

Blockchain technology has great potential in the field of finance, particularly in the area of transparent audits. Conventional auditing procedures are sometimes lengthy and susceptible to mistakes made by humans. These procedures typically include numerous parties with potentially competing interests. Blockchain implements an unchangeable ledger system, where every transaction is recorded in a certain order and cannot be modified afterwards. This functionality guarantees the permanent storage and universal accessibility of documents, which facilitates immediate auditing and minimizes the chances of fraudulent activities. Financial institutions may enhance the efficiency and comprehensiveness of financial data verification by implementing smart contracts, which automate these operations and enable continual and transparent audits [60].

In addition, the technology behind blockchain improves risk assessment. In the field of finance, evaluating and managing risk requires complex computations that make use of enormous datasets. These computations frequently require inputs from a wide variety of sources, some of which may not

 doi:10.20944/preprints202407.1977.v1

always give information that is reliable or up to date. By providing analysts with a centralized and trustworthy source of data, blockchain technology has the potential to make these difficulties more manageable. Access in real time to the financial activities of borrowers that are recorded on a blockchain has the potential to significantly enhance credit risk assessment. This method not only improves the effectiveness of the risk assessment process, but it also reduces the likelihood of credit defaults by making it easier to make decisions that are both more accurate and more rapid [61].

Additionally, the use of blockchain technology has brought about considerable benefits to the administration of compliance in the banking industry. In general, financial institutions are required to comply with regulatory requirements, which include the creation and maintenance of open and accessible records, the execution of comprehensive reporting, and the assurance of the data's integrity and safety. Because of its decentralized nature, blockchain technology makes it possible to create systems that ensure compliance data is both secure and regularly updated. These systems also allow regulators to verify compliance data without the need for intermediaries to have to be involved [62]. This function significantly cuts down on the amount of time and resources needed for compliance management, and it has the potential to significantly enhance the accuracy of the reports that are filed.

To effectively apply blockchain technology in several fields of finance, issues including scalability, integration with present technologies, and the development of industry-wide standards have to be resolved first. Still, the creation of these blockchain uses in the financial sector is a commendable endeavor given the possible advantages from more transparency, better efficiency, and more security. As this technology develops constantly, it is highly likely that it will finally become a necessary part of the process of upgrading financial institutions around the world.

6.2. Supply Chain Management

The implementation of blockchain technology has the potential to greatly improve the capacity to track and ensure responsibility in the management of supply chains. Efficiency and dependability in complicated supply chains depend on the provenance of commodities, real-time tracking of their movement, and openness in production processes. The decentralized and irreversible characteristics of blockchain offer a unique solution to these difficulties by providing a transparent method for documenting and validating each stage of the supply chain process [63].

The implementation of blockchain technology in supply chain management fundamentally revolutionizes the process of gathering and disseminating information among different entities involved, such as suppliers, manufacturers, distributors, and retailers. Blockchain enables the establishment of a collective, unchangeable record, guaranteeing that every transaction or transfer of products is documented in a way that is both transparent and verifiable by all involved parties [64]. This openness facilitates the establishment of a singular and reliable source of information, hence minimizing the occurrences of disagreements and the necessity for intermediaries who have historically been involved in managing these interactions.

Managing the logistics of perishable commodities, high-value items, or anything that raises ethical or legal questions calls especially for traceability. Blockchain technology allows one to track products from the point of origin all the way to the final buyer, instantly. This guarantees that every good can be traced back to its source [65]. This degree of traceability guarantees compliance with legal obligations, helps to enforce quality control standards, and verifies the validity of items, thereby benefiting various aspects. Beginning with its source on the farm and finishing with its final destination with the client, blockchain technology has the potential to be used in the food sector for the aim of correctly monitoring the full supply chain of a good. The use of this system might significantly improve safety criteria and enable quick reaction in case of any issues, including contamination.

The adoption of blockchain equally enhances accountability. Accountability is frequently compromised in conventional supply chains because of the lack of transparency in operations and the challenge of identifying responsibility when differences occur. The blockchain guarantees that every activity performed by a participant is meticulously documented [66]. This facilitates the

 doi:10.20944/preprints202407.1977.v1

identification of liable entities and the enforcement of responsibility in instances of failure to adhere to established norms or regulatory obligations. Furthermore, the unchangeability of blockchain records inhibits tampering, rendering it a potent instrument for preventing fraud and guaranteeing that all parties comply with the conditions of their contractual commitments.

In spite of these advantages, the use of blockchain technology in supply chain management necessitates the overcoming of significant challenges that arise, such as the incorporation of blockchain technology into existing information technology systems, the scalability of the technology, and the development of universal standards to ensure interoperability among multiple stakeholders. It is also necessary for organizations to undergo cultural transformations in order to accommodate this high level of transparency and shared control.

6.3. Healthcare

Blockchain technology in the healthcare industry offers a novel method of decentralized decision-making in managing patient data and conducting medical research. It revolutionizes the way data is kept, exchanged, and utilized among many parties involved, such as healthcare professionals, patients, and researchers. The use of blockchain enables a transition from conventional centralized data management systems, which can entail substantial bureaucratic burdens and certain weaknesses, to a more secure, transparent, and efficient decentralized framework [67].

The decentralized feature of blockchain is highly advantageous in the administration of patient data. Within this system, medical records are distributed throughout a network of nodes, therefore preventing centralization and reducing vulnerability to cyberattacks and illegal access. Every record on a blockchain is marked with a timestamp and connected to preceding records, forming an immutable historical data sequence. The inherent immutability of blockchain guarantees that once medical information is documented, it is impossible to alter or erase, hence preserving the integrity of medical data. Moreover, blockchain technology enables patients to have enhanced authority over their own medical data. By utilizing cryptographic keys for access control, patients have the ability to grant or withdraw data access to healthcare practitioners, researchers, or other parties [68]. This process enables patient-centered decision-making. Such a high degree of control not only improves the protection of patient confidentiality but also increases confidence in the healthcare system, since patients are aware that their data is being handled safely and with their explicit permission.

Blockchain has the potential to significantly transform the sharing and utilization of data in medical research as well. The system enables the secure collection of health data from many sources while preserving patient privacy, therefore facilitating more comprehensive research projects that need extensive databases. Accessing de-identified patient data allows researchers to obtain a substantial amount of information without violating the privacy of individuals. This enables faster research procedures and promotes the advancement of tailored treatment. Blockchain also tackles substantial obstacles in clinical studies. It may be utilized to monitor the status of permission forms, guaranteeing their currency and integrity [69]. In addition, blockchain enables the continuous monitoring of clinical trial methods and outcomes, so enhancing the transparency and dependability of study findings. This feature not only aids in adhering to regulatory mandates but also enhances the trustworthiness of the completed study.

Despite this, applying blockchain technology in the healthcare sector calls for the overcoming of certain obstacles. Ensuring that the technology is scalable enough to handle the significant volume of data usually found in healthcare environments, building a regulatory framework that especially addresses the unique qualities of blockchain in healthcare, and encouraging a cultural change that makes it simpler for healthcare professionals and institutions to accept blockchain technology, serve as significant challenges, among many others [70].

6.4. Government and Public Sector

Blockchain technology has the potential to significantly improve the transparency, security, and efficiency of voting systems and the administration of public documents in the government and public sector. Through utilizing the decentralized and unchangeable characteristics of blockchain

 doi:10.20944/preprints202407.1977.v1

technology, governments may effectively tackle enduring issues pertaining to trust and integrity in public administration [71].

Blockchain has the potential to radically alter the conduct of elections, enhancing both security and accessibility in the voting process. Conventional voting methods frequently encounter problems including voter fraud, manipulation of ballots, and a lack of openness, all of which can undermine public confidence in political procedures. Blockchain-based voting systems utilize the blockchain technology to record votes as transactions, guaranteeing that once a vote is submitted, it is immutable and cannot be modified or removed. The immutability of each vote guarantees its integrity. Furthermore, the use of blockchain technology enables voters and oversight groups to confirm the accuracy of vote recording and counting, while preserving the anonymity of voters and ensuring the confidentiality of the ballot. Another benefit of utilizing blockchain technology in voting is its ability to enable distant and electronic voting. Blockchain technology can facilitate voting by employing cryptographic methods to ensure security. This allows voters to cast their votes using personal devices like smartphones or laptops, therefore minimizing the logistical challenges and expenses typically associated with conventional voting approaches. This kind of accessibility can result in a higher voter participation rate, particularly in geographically isolated or underserved regions, as well as in situations where in-person voting is challenging, such as during pandemics [72].

Apart from voting, blockchain technology presents significant improvements in the way public documents are being managed. Government records—which cover property titles, licenses, educational background, and health information—demand strict security and authenticity to prevent fraud and build public and other governmental entity confidence. Blockchain is ideal for managing these kind of records as it provides a safe, transparent, unchangeable ledger. Incorporating blockchain technology into public records handling helps to create a consistent and trustworthy transaction record. Authorized people might be able to view this material under protection against unlawful access and alteration. This system improves public service delivery's efficiency and accuracy, reduces the administrative load connected to record keeping, and lowers the potential of data loss or corruption. Furthermore, by providing a shared platform that permits safe and real-time access to records, blockchain technology can improve inter-agency cooperation. This, in turn, improves the government operations' efficiency [73].

Nevertheless, all of these advantages aside, the use of blockchain technology in governmental contexts continues to present difficulties. These include the necessary technological competence for the construction and operation of blockchain systems, the crucial requirement for considerable investments in infrastructure, and the design of legislation that address concerns related to privacy, security, and ethics that are linked with digital governance. In addition, there is a cultural factor that has to be taken into consideration, as citizens and public officials alike are required to completely embrace the revolutionary changes that blockchain technology has brought about.

6.5. Energy Sector

The use of blockchain technology into the energy industry, namely in the management of distributed energy resources and smart grids, signifies a significant transition towards more decentralized and efficient energy systems. The ability of blockchain to optimize operations, improve transparency, and ensure safe data transmission is well-suited to the requirements of contemporary energy networks, which heavily depend on a variety of energy supplies spread across different locations [74].

Distributed energy resources (DERs), such as solar panels, wind turbines, and battery storage systems, provide distinct difficulties for energy management due to their fluctuating nature, decentralized nature, and the requirement for meticulous coordination. Conventional centralized energy management systems frequently face challenges in effectively incorporating several small-scale, sporadic energy sources. Blockchain technology provides a possible answer by enabling secure and real-time communication and transaction capabilities across a distributed network [75].

Blockchain allows for a decentralized approach to energy management within the framework of smart grids. Smart grids, which utilize digital communication technologies to identify and respond

 doi:10.20944/preprints202407.1977.v1

to local fluctuations in consumption, can derive several advantages from blockchain. Blockchain may be utilized to establish a safe and transparent platform for energy trade transactions. In the context of peer-to-peer (P2P) energy trading, houses equipped with solar panels have the ability to directly sell any surplus electricity to nearby residents or other interested parties, without the involvement of conventional energy providers as intermediaries. This not only improves efficiency by decreasing transmission losses linked to distant energy sources but also promotes the utilization of renewable energy by making it more economically feasible and advantageous for producers. Furthermore, blockchain enables enhanced demand response tactics inside smart grids. Blockchain ensures the integrity and permanence of data exchanges, creating a dependable and precise database that captures energy use trends. Utility companies may utilize this data to enhance their capacity to forecast increases in demand and make necessary adjustments to supply, a critical factor in ensuring grid stability and optimizing energy distribution. Furthermore, blockchain technology can facilitate the implementation of flexible pricing models that respond to changes in power supply and demand [76]. This encourages consumers to decrease their use during high-demand periods or move it to times when demand is lower.

Blockchain technology offers capabilities that can affect cybersecurity as well as regulatory compliance in the energy sector. When it comes to meeting high regulatory criteria for transparency and reporting, the inherent qualities of the technology—which include data integrity, traceability, and security—are rather crucial. Furthermore, by stopping illegal access and data manipulation, blockchain technology enhances the cybersecurity of smart grids. This protects smart grids against probable flaws and hazards that can disturb the supply and distribution of power [77].

6.6. Case Studies and Real-World Examples

When examining the influence of blockchain on decentralized decision-making, several practical instances emerge, showcasing the technology's revolutionary capacity in different industries. These case studies showcase both successful implementations and offer significant insights into the difficulties and advantages of incorporating blockchain into intricate systems.

An excellent example is the utilization of blockchain technology in the financial industry by the Australian Securities Exchange (ASX). ASX is undertaking a bold initiative to replace its current system for handling equities transactions with a system based on blockchain technology. The objective is to save expenses, improve transparency, and optimize post-trade procedures. This technology, created in partnership with Digital Asset Holdings, utilizes the unchangeable and transparent nature of blockchain to offer immediate data access to all market players. It also guarantees the reliability and protection of financial records. This move signifies an early and significant implementation of blockchain technology by a national securities exchange, establishing a model for other entities in the financial sector. Figure 16 visualizes ASX's architecture.

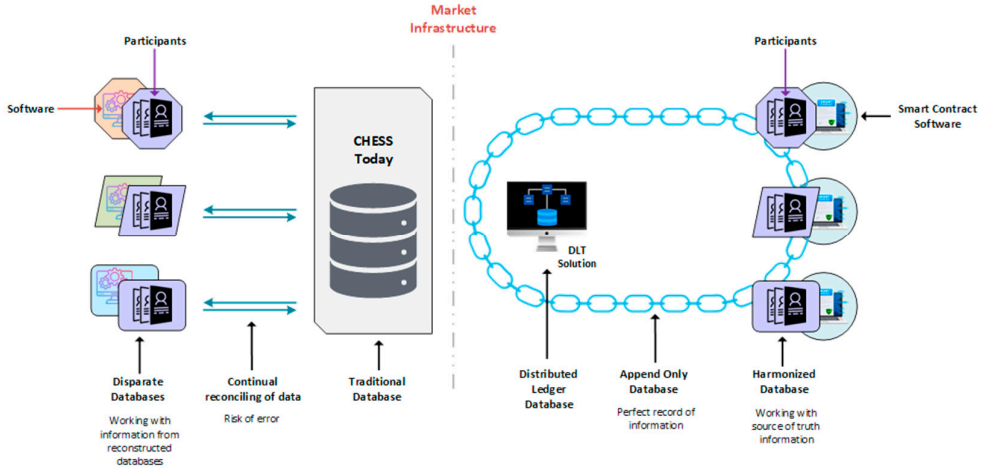

Figure 16. Architecture of Australian Securities Exchange (ASX).

 doi:10.20944/preprints202407.1977.v1

Another demonstration of the vast potential of blockchain technology, which is to increase the ability to track and assure responsibility in the flow of commodities is provided by the partnership between Walmart and IBM on the Food Trust Blockchain project, which has its roots in the field of supply chain management. The purpose of this initiative is to track the provenance of food products from the point of origin all the way to the point of sale. The project makes it possible to have a clear and unobstructed awareness of the supply chain, which in turn makes it possible to quickly identify things that may be contaminated. This results in a significant decrease in the amount of time and money that is required to carry out food safety inspections and recalls. The utilization of blockchain technology not only improves the safety of customers, but it also maximizes the effectiveness of supply chain operations by reducing waste and improving product management across the board everywhere. Figure 17 shows the way Walmart's and IBM's Food Trust Blockchain Project works.

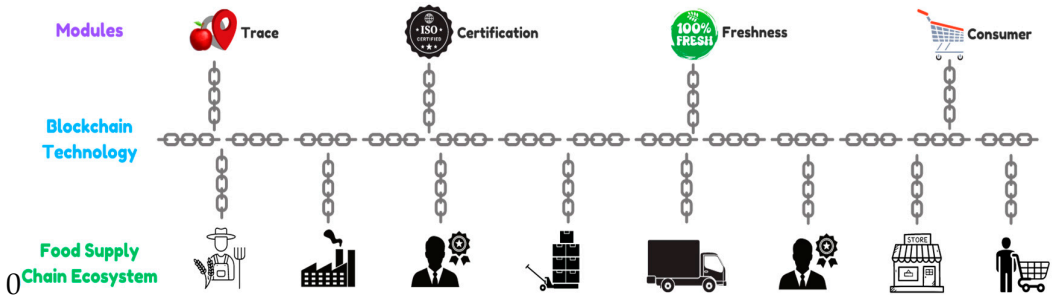

Figure 17. Walmart's and IBM's Food Trust Blockchain Project.

The Brooklyn Microgrid program is a fascinating example of a case study in the field of energy distribution. This project makes use of blockchain technology to monitor and record energy transactions that take place within a localized microgrid. As a result, it gives communities the ability to buy and sell green energy through direct transactions with one another. The implementation makes use of blockchain technology to provide a platform for energy transactions that is both extremely secure and decentralized. This eliminates the need for a traditional utility company to act as a middleman in the transaction process. This not only provides clients with increased control, but it also encourages the usage of renewable energy sources by making energy trading widely accessible and financially practical for smaller producers. Figure 18 depicts in a simple way the architecture behind the Brooklyn Microgrid Project.

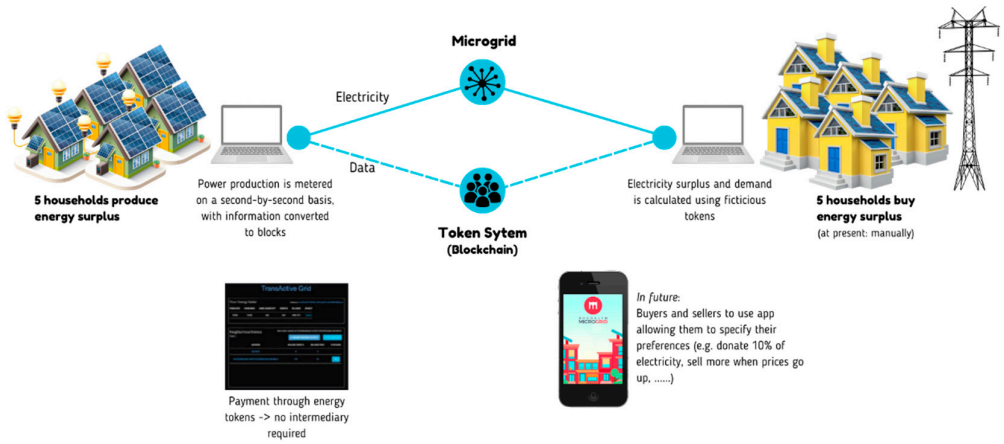

Figure 18. The Brooklyn Microgrid Project.

In order to guarantee the distributed and safe administration of patient health records, Estonia has been a leading example in using blockchain technologies in healthcare. Working with Guardtime, Estonia has effectively used blockchain technology to protect around a million health records. Every

 doi:10.20944/preprints202407.1977.v1

incident involving accessing patient data is permanently recorded by the system, therefore producing an unambiguous record of events that discourages illegal data access and improves the consistency and accuracy of the data. Security and confidentiality of sensitive data may be enhanced by the use blockchain technology, as this application shows so far, which is an important feat in the healthcare sector. Figure 19 shows how Estonia's EHR system works after collaborating with Guardtime.

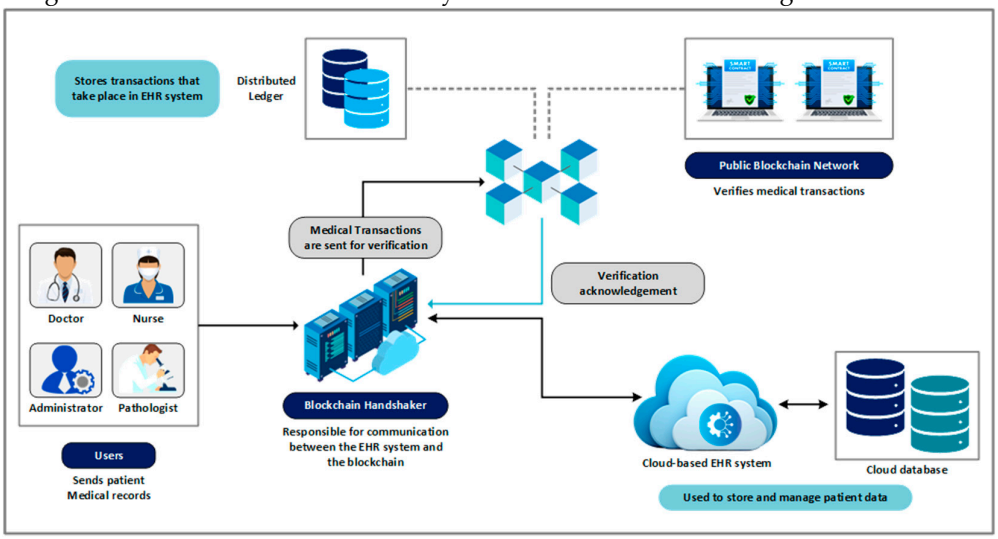

Figure 19. Estonia's partnership with Guardtime, the EHR System.

These real-life cases demonstrate that although the uses of blockchain might vary greatly, the fundamental advantages - heightened transparency, greater security, and improved efficiency - are constant. Nevertheless, these implementations also emphasize prevalent challenges, such as the requirement for substantial initial capital, the intricacy of incorporating blockchain with current systems, and the continuous necessity to handle scalability and performance concerns. Every case presents a crucial chance for other firms contemplating blockchain to gain valuable insights. Through the examination of these accomplished implementations, stakeholders may gain a deeper understanding of how to utilize the advantages offered by blockchain while also mitigating its drawbacks. This will enable them to make more knowledgeable and efficient use of the technology in decentralized decision-making across different fields.

7. Big Data and Blockchain in Decision-Making

Any possible chance for decentralized decision-making processes in a variety of sectors is presented by the combination of Big Data with blockchain technology, which provides a revolutionary opportunity [78]. Through the utilization of the benefits offered by both technologies, businesses have the potential to enhance data security, transparency, and efficiency, which ultimately leads to decisions that are more reliable and well-informed. The process of decentralized decision-making involves the distribution of decision-making authority across several nodes or participants within a network, as opposed to relying on a single authority to make decisions. The efficiency of this strategy is significantly improved when combined with blockchain technology and big data. Big Data provides access to enormous databases as well as analytical tools, all of which are of critical importance when it comes to gaining insights and making decisions. Blockchain technology simultaneously ensures the confidentiality, authenticity, and openness of the data that is being employed [79]. Collectively, they offer a decision-making process that is more inclusive, adaptive, and efficient. This method enables rapid and informed choices to be made based on real-time data, while also assuring security and dependability.

 doi:10.20944/preprints202407.1977.v1

7.1. Enabling Real-Time Data Processing and Decision-Making in Decentralized Systems

The integration of Big Data analytics with blockchain technology significantly enhances real-time data processing and decision-making in decentralized systems. By leveraging blockchain's distributed ledger, multiple nodes can securely share and process data simultaneously. This decentralized approach ensures that decisions are based on the most current and accurate information, enabling more efficient and informed outcomes. Furthermore, the use of smart contracts can automate these processes, reducing latency and improving overall system responsiveness [80].

Big data analytics rely on the ability to effectively manage large volumes of data and draw important insights. In distributed systems when data is constantly produced from several sources, this capability is absolutely vital. Blockchain technology provides a distributed architecture allowing immediate data exchange and processing among numerous nodes, hence enabling this feature. Blockchain permits direct peer-to-peer data flow unlike centralized systems, which depend on data to pass a central authority. The distributed approach lets faster and more efficient decision-making possible by lowering the congestion resulting from centralized data processing systems [81].

Blockchain combined with Big Data analytics has the ability to drastically change financial services real-time decision-making procedures. Blockchain's distributed ledger lets all of the nodes quickly record and verify financial transactions. Big Data analytics systems then may quickly review these transactions, closely looking for patterns and anomalies that would indicate prospective dangers or fraudulent activity. By quickly responding to such attacks, financial companies can achieve less losses and improve general security [82].

In addition, in decentralized supply chain networks, the utilization of blockchain and Big Data for real-time data processing is essential for enhancing operational efficiency. Blockchain offers a clear and unchangeable record of all transactions and movements inside the supply chain. Big Data analytics can analyze this data in real-time, offering valuable insights into inventory levels, shipping statuses, and any interruptions. The ability to see current information immediately enables supply chain managers to make well-informed choices quickly, such as redirecting shipments or modifying inventory levels [83]. This improves efficiency and lowers expenses.

The integration of blockchain and Big Data in the healthcare industry facilitates the immediate administration of patient data and enhances the process of making informed decisions. Authorized healthcare practitioners across several regions can access patient records stored on a blockchain, guaranteeing access to the most current information. Big Data analytics may analyze this data to offer immediate insights into patient health, forecast probable issues, and suggest customized treatment strategies. The capacity to provide information in real-time is especially advantageous in emergency scenarios, as it can potentially save loss of life by delivering fast and precise data [84].

In addition, in order to achieve a balance between supply and demand, real-time data processing is a crucial component of decentralized models of energy management. The technology known as blockchain has the capability to record data on energy production and consumption in real time from a wide variety of distributed energy resources (DERs). Once this data has been collected, Big Data analytics may be used to evaluate it in order to estimate demand, improve energy distribution, and uncover potential for energy savings. This feature enables the effective functioning of smart grids, which guarantees a consistent and dependable supply of electricity while simultaneously reducing prices and the number of negative effects on the environment [85].

The decentralized nature of blockchain technology improves the safety and dependability of real-time data processing. Every node in the network keeps a copy of the blockchain, which ensures that the data is redundant and reduces the likelihood that the data will be lost or corrupted by any means. The resilience of the system is improved by this distributed method, which allows it to continue to function successfully even in the event that any of the nodes are compromised or that they become down.

7.2. Facilitating Predictive Analytics and Automation

One of the main benefits of combining Big Data analytics with blockchain technology, especially in the context of distributed decision-making, is that it facilitates predictive analytics and automation.

 doi:10.20944/preprints202407.1977.v1

Using predictive analytics—that is, leveraging both historical and real-time data to project future trends and outcomes—allows distributed decision-making approaches great benefits. Blockchain technology assures the validity and reliability of the examined data, therefore improving this process. Also, smart contracts help to simplify the decision-making process by automating it [86].

7.2.1. Predictive Analytics in Decentralized Systems

Predictive analytics use extensive information to detect patterns, trends, and correlations that might offer valuable insights into forthcoming occurrences. Data quality and dependability are of utmost importance in decentralized systems. Blockchain technology guarantees the security, accuracy, and immutability of the data utilized for predictive analytics. Every piece of data entered into a blockchain is unchangeable and marked with a timestamp, resulting in a reliable historical record that predictive models may depend on [87].

In a decentralized supply chain network, blockchain has the capability to document and track each transaction and movement of commodities. Subsequently, Big Data analytics may utilize this past data to forecast variations in demand, anticipated interruptions in the supply chain, and the most advantageous levels of inventory. Predictive models utilize historical data trends to provide projections, enabling stakeholders to make well-informed decisions regarding production schedules, shipping routes, and inventory management. This ultimately improves the efficiency and resilience of the supply chain [88].

Lastly, the application of predictive analytics in the financial industry allows for the forecasting of market movements, the evaluation of credit risks, and to identify fraudulent actions. The transactional data that is utilized in these studies is guaranteed to be inaccurate and unchangeable thanks to blockchain technology. Identifying investment possibilities, managing risks, and improving compliance with regulatory requirements are all things that may be accomplished with the use of predictive models by financial institutions. It is possible to make proactive decisions thanks to this predictive power, which in turn helps to reduce the likelihood of prospective losses and improve financial performance.

7.2.2. Enhancing Decision-Making with Predictive Analytics and Automation

Improvements in decentralized decision-making are made possible by the integration of predictive analytics and automation through smart contracts. These improvements include the provision of timely, data-based insights and the autonomous execution of choices. This collaboration not only ensures that decisions are made based on the most accurate and up-to-date information, but it also makes the process of putting these decisions into action more effective [89].

It is possible, for example, to use predictive analytics in a decentralized logistics network in order to estimate delivery timeframes and identify any delays that may occur. Because smart contracts have the potential to autonomously reroute shipments, adjust delivery schedules, and communicate with necessary parties, they ensure that logistical activities are carried out in a manner that is both efficient and effective. The deployment of this automated decision-making capability in real-time leads to a reduction in operational dangers and an improvement in overall performance. All of these benefits are achieved simultaneously.

8. Challenges and Potential Issues in Integrating Big Data and Blockchain for Decentralized Decision-Making

In order to successfully capitalize on the benefits of integrating Big Data with blockchain technology for decentralized decision-making, it is necessary to solve several obstacles and potential concerns. These obstacles encompass technological, operational, and regulatory aspects, and it is vital to tackle them in order to achieve effective implementation and long-term viability of these technologies.

 doi:10.20944/preprints202407.1977.v1

Scalability and Performance

When it comes to combining blockchain technology with big data, scalability is one of the most significant problems. Both of these technologies are naturally associated with huge transaction volumes and enormous databases itself. When it comes to blockchain networks, particularly those that are based on Proof of Work (PoW) consensus processes, blockchain networks frequently experience low transaction throughput and significant latency. When it comes to processing massive volumes of data in real time, which is absolutely necessary for Big Data analytics, this can easily become a bottleneck. In a similar vein, Big Data systems need comprehensive infrastructure in order to manage the processing and storage of massive amounts of data. When blockchain technology is included, an additional layer of complexity is added since every transaction must be logged on the blockchain. This might possibly slow down the processing speed. It is still a big problem to ensure that both systems are able to grow effectively in order to manage rising data loads and transaction volumes without compromising performance [90].

Several cutting-edge technologies and frameworks are being developed to address these scalability issues. For example, sharding is a method where the blockchain is partitioned into smaller, more manageable pieces called shards. Each shard can process transactions independently, significantly increasing the overall transaction throughput. Another solution is the implementation of layer-two protocols, such as the Lightning Network for Bitcoin, which allows for off-chain transactions that are later settled on the main blockchain, reducing congestion and improving speed.

Data Privacy and Security

Although blockchain improves data security by using an immutable and transparent ledger, it also raises privacy issues. Within a decentralized decision-making setting, the possibility arises that sensitive material might be accessed by several participants, leading to concerns over the confidentiality of the data. While blockchain employs cryptographic methods to safeguard data, the inherent transparency of blockchain can occasionally clash with the imperative for privacy, particularly in industries such as healthcare and finance where data confidentiality is of the utmost importance for patients and clients alike [91].

Ensuring data privacy while maintaining transparency and auditability is a delicate thread that we have to walk on. Techniques such as zero-knowledge proofs and homomorphic encryption are being explored to enhance privacy on blockchain platforms. Zero-knowledge proofs allow one party to prove to another that they know a value without revealing the value itself. Homomorphic encryption enables computations to be carried out on encrypted data without needing to decrypt it first, ensuring data privacy throughout the process [92]. These solutions are still in developmental stages but hold significant promise for maintaining privacy in blockchain-integrated systems.

Interoperability and Integration

Blockchain integration with current Big Data platforms and infrastructure presents serious interoperability problems. Most companies have already set up data management systems; adding blockchain calls for smooth integration to guarantee continuity and efficiency. This involves not just technological compatibility but also harmonizing the data formats, protocols, and standards across different systems. Furthermore, of great importance is the interoperability feature across several blockchain systems themselves. Transferring data and assets across platforms is difficult, as different blockchains apply different consensus mechanisms and data types [93].

Efforts are being made to develop standardized protocols and frameworks that facilitate interoperability between blockchain networks and traditional systems. Projects like Polkadot and Cosmos are designed to enable different blockchains to communicate and share information, creating an internet of blockchains. Additionally, middleware solutions that act as bridges between blockchain and legacy systems are being developed to streamline integration processes.

Regulatory and Compliance Issues

The legislative framework for blockchain and Big Data is still evolving, as many countries have challenges in keeping up with the fast progress of these technologies. Adhering to data protection regulations like GDPR in Europe and CCPA in California presents further difficulties. The unchangeable nature of blockchain poses challenges in adhering to legislation that mandate the

 doi:10.20944/preprints202407.1977.v1

modification or deletion of data upon request. Furthermore, decentralized decision-making sometimes lacks well-defined regulatory frameworks, resulting in uncertainty and possible legal liabilities. Organizations must effectively manage complex regulatory frameworks to guarantee that their utilization of blockchain and Big Data adheres to both local and international legal requirements, a process that may be demanding in terms of resources and complexity [94].

To address regulatory compliance issues, hybrid blockchain models are being explored. These models combine the benefits of public and private blockchains, allowing for controlled access and compliance with regulatory requirements. Moreover, regulatory sandboxes are being used to test and refine blockchain applications within a controlled environment before full-scale deployment. These sandboxes enable developers to understand and navigate regulatory frameworks better, ensuring that their solutions are compliant.

Cost and Resource Allocation

Implementing solutions based on blockchain technology and big data can be expensive since it requires a considerable investment in hardware, software, and individuals with the necessary skills. A significant amount of financial resources are required for the initial setup, ongoing maintenance, and continuously upgraded versions of these systems. Additionally, an equally significant problem is the amount of energy that is used by blockchain technology, particularly by systems that are based on proof-of-work. It is exceedingly important for organizations, particularly those with restricted resources, to strike a balance between the expenses and the projected benefits. In addition, the situation is made even more difficult by the dearth of individuals that are knowledgeable in both blockchain technology and Big Data experience. The training of current personnel or the employment of new talent with the necessary abilities is very important, but it can be both time-consuming and potentially expensive [95].

Transitioning to more energy-efficient consensus mechanisms, such as Proof of Stake (PoS) or Delegated Proof of Stake (DPoS), can help reduce costs associated with energy consumption. Additionally, cloud-based blockchain services offered by companies like IBM and Microsoft provide scalable and cost-effective solutions that can help organizations manage their resources more efficiently. These services allow organizations to leverage blockchain technology without the need for significant upfront investment in infrastructure.

Governance and Consensus

Having strong governance and processes for reaching agreement are essential to the success of decentralized decision-making. A decentralized network has a number of challenges, one of which is ensuring that all members can establish agreement in an efficient and equitable manner. There is a possibility that various stakeholders will have different interests and motivations, which might result in disagreements and delays in decision-making. The models of governance need to be created in such a way that they guarantee inclusiveness, transparency, and efficiency while also limiting the accumulation of power in the hands of a small number of participants. In addition, the complexity of consensus methods like PoS, DPoS, and PBFT need a comprehensive understanding of these techniques as well as their appropriate implementation in order to prevent vulnerabilities and guarantee the stability of the network [97].

Innovative governance models, such as decentralized autonomous organizations (DAOs), are being developed to address these challenges. DAOs use smart contracts to automate decision-making processes and ensure that all stakeholders have a voice in governance. Additionally, research into consensus algorithms, such as Byzantine Fault Tolerance (BFT) and its variations, aims to improve the efficiency and fairness of reaching consensus in decentralized networks.

To sum it up, the combination of blockchain technology and Big Data presents great chances to improve distributed decision-making procedures. To really leverage their advantages to the fullest, however, various challenges and possible problems must be resolved. Important aspects that need great thought and creative ideas include scalability, data privacy, interoperability, regulatory compliance, pricing, resource allocation, and governance. By addressing these challenges, companies may build strong, effective, and safe distributed decision-making systems, while leveraging

 doi:10.20944/preprints202407.1977.v1

blockchain technology's advantages as well as Big Data's. Figure 20 summarizes the issues presented above in integrating Big Data and Blockchain for decentralized decision-making purposes.

Table 6. A summary of Challenges in integrating Big Data and Blockchain for decentralized decision-making.

Type	Summary
Scalability and Performance	Integrating Big Data and blockchain faces scalability issues due to large datasets and high transaction volumes. Blockchain networks, particularly those using Proof of Work (PoW), have limited transaction throughput and high latency, which can slow down data processing. Solutions like sharding and layer-two protocols are being developed to improve scalability and performance.
Data Privacy and Security	Blockchain enhances data security but poses privacy concerns due to its transparency. Ensuring data confidentiality in sectors like healthcare and finance is challenging. Techniques like zero-knowledge proofs and homomorphic encryption are being explored to balance privacy and transparency.
Interoperability and Integration	Integrating blockchain with existing Big Data systems presents interoperability challenges, requiring seamless technical compatibility and alignment of data formats and protocols. Efforts are underway to develop standardized protocols and middleware solutions to facilitate integration and interoperability between blockchain networks and traditional systems.
Regulatory and Compliance Issues	The evolving regulatory landscape for blockchain and Big Data presents challenges in compliance with data protection laws. Blockchain's immutable nature conflicts with regulations requiring data modification or deletion. Hybrid blockchain models and regulatory sandboxes are being explored to ensure compliance while leveraging blockchain technology.
Cost and Resource Allocation	Implementing blockchain and Big Data solutions is costly, requiring significant investment in hardware, software, and skilled personnel. Energy consumption, particularly in PoW systems, is a major concern. Transitioning to energy-efficient consensus mechanisms and using cloud-based blockchain services can help manage costs and resources.
Governance and Consensus	Effective governance and consensus mechanisms are crucial for decentralized decision-making. Ensuring inclusivity, transparency, and efficiency while preventing power concentration is challenging. Innovative governance models like decentralized autonomous organizations (DAOs) and research into consensus algorithms aim to improve decision-making processes and network stability.

9. Future Directions and Emerging Trends

Originally created to support Bitcoin, blockchain technology has now developed into a fundamental technology with the capacity to revolutionize other sectors. This section will present an overview of how blockchain has evolved from being a facilitator of digital currency to being a widely influential and transformative technology. Stakeholders must comprehend and predict upcoming trends in order to maintain a competitive edge in technological improvements and use blockchain's whole potential in inventive and influential manners.

As the blockchain technology advances, substantial attempts are being undertaken to tackle its inherent constraints, including scalability and transaction velocity. Technological advancements such

 doi:10.20944/preprints202407.1977.v1

as sharding, which involves dividing the network into smaller and more manageable sections, and layer-two solutions like the Lightning Network, which enables transactions to occur outside the main blockchain, play an important part in improving the scalability of blockchain technology. In addition, sidechains are being created to enhance the interoperability of blockchains, enabling a more efficient and interconnected network. These technological breakthroughs are essential for the widespread acceptance and implementation of blockchain technology worldwide.

The integration of blockchain with advanced technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and quantum computing is creating opportunities for revolutionary applications in several industries. Artificial intelligence (AI) may be employed to streamline and improve the efficiency of blockchain operations and augment the capabilities of smart contracts. At the same time, blockchain technology can bolster the security and ensure the integrity of data transmitted by Internet of Things (IoT) devices within a networked setting. In addition, when quantum computing emerges, blockchain is making preparations to counter possible security risks by implementing quantum-resistant cryptographic techniques, thereby guaranteeing its long-term survival as a secure digital ledger.

Blockchain technology is anticipated to bring about a significant transformation in the financial industry as well, by enabling advancements in programmable currency and decentralized finance (DeFi). These innovations eliminate the need for middlemen in financial transactions, resulting in reduced expenses and improved effectiveness. Blockchain technology has the potential to greatly improve transparency and decrease carbon footprints in supply chain management by allowing for more accurate monitoring of commodities and their environmental consequences. Blockchain technology also has the potential to revolutionize the healthcare industry by facilitating sophisticated patient data management systems and enabling the worldwide sharing of health data. This might lead to improved diagnostics and treatments.

As the use of blockchain technology becomes more widespread, it needs to conform to worldwide legislative frameworks that are specifically meant to safeguard privacy, such as the General Data Protection Regulation (GDPR) in Europe. Furthermore, it is crucial to prioritize the ethical utilization of blockchain to guarantee that when blockchain technologies grow widespread, they uphold data sovereignty and personal rights. This involves overseeing the equilibrium between transparency and confidentiality, and guaranteeing that blockchain deployments do not unintentionally result in heightened monitoring or authority over individuals.

Nonetheless, blockchain also presents several challenges to its widespread adoption even if it has huge potential. Technical challenges include energy consumption and the complex integration with present systems, which must be addressed first. Furthermore, cultural opposition and unclear laws might hinder acceptance of it. Moreover, there is growing need for qualified professionals with strong knowledge of blockchain technology to properly enable its implementation across several sectors. General acceptance and prosperity of blockchain technology depend on their overcoming of these challenges.

10. Conclusions

The integration of Big Data and blockchain technology represents a significant leap forward for decentralized decision-making across various industries. This comprehensive review has explored how these two powerful technologies intersect, examining their combined benefits, challenges, and real-world applications.

Blockchain technology, with its decentralized, immutable ledger, provides a secure and transparent framework for data management. Its ability to ensure data integrity and prevent unauthorized tampering makes it an ideal partner for Big Data, which is characterized by the five V's: volume, velocity, variety, veracity, and value. By leveraging blockchain's strengths, organizations can enhance the reliability and security of their Big Data initiatives.

Big Data analytics, on the other hand, offers the tools needed to process and analyze vast amounts of data in real time, extracting meaningful insights that drive informed decision-making.

 doi:10.20944/preprints202407.1977.v1

When integrated with blockchain, these analytics can operate on a more secure and trustworthy data foundation, ensuring that decisions are based on accurate and untampered information.

This synergy between Big Data and blockchain facilitates several key advantages. Enhanced data security and integrity are crucial for maintaining the trustworthiness of information used in decision-making. Improved transparency and traceability allow organizations to track data provenance and ensure authenticity, which is particularly valuable in supply chain management and other sectors where tracking the origin and journey of products is essential. Real-time data processing capabilities enable swift responses to emerging trends and threats, while predictive analytics and automation streamline decision-making processes, making them more efficient and reliable.

Despite these promising benefits, integrating Big Data and blockchain technology is not without its challenges. Scalability issues, data privacy concerns, interoperability hurdles, regulatory compliance complexities, high implementation costs, and the need for skilled professionals are significant obstacles that need to be addressed. By focusing on innovative solutions to these challenges, organizations can unlock the full potential of these technologies.

The real-world applications and case studies highlighted in this paper, such as Estonia's blockchain-based healthcare system, IBM and Walmart's Food Trust blockchain platform, and the Brooklyn Microgrid project, demonstrate the transformative impact of integrating Big Data and blockchain. These examples showcase how these technologies can enhance data security, transparency, and operational efficiency, driving innovation and improving outcomes in healthcare, supply chain management, and energy sectors.

Looking ahead, the continued evolution of Big Data and blockchain technology promises even greater advancements in decentralized decision-making. Future research and development will be crucial in addressing current limitations and exploring new applications across various industries. By staying at the forefront of these technological developments, organizations can leverage the full potential of Big Data and blockchain to create more secure, efficient, and reliable decision-making systems.

Author Contributions: Conceptualization, L.T.; methodology, L.T.; software, A.T.; investigation, A.T.; resources, L.T.; writing—original draft preparation, A.T.; writing—review and editing, L.T.; visualization, A.T.; supervision, C.H.; project administration, C.H.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Schinckus, C. (2020). The good, the bad and the ugly: An overview of the sustainability of blockchain technology. Energy Research & Social Science, 69, 101614. [CrossRef]
2. Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. Journal of King Saud University-Computer and Information Sciences, 34(9), 6719-6742. [CrossRef]
3. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee. [CrossRef]
4. Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., ... & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. Ieee Access, 9, 61048-61073. [CrossRef]
5. Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067. [CrossRef]
6. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and sustainable energy reviews, 100, 143-174. [CrossRef]
7. Malek, S., Mikic-Rakic, M., & Medvidovic, N. (2005, November). A decentralized redeployment algorithm for improving the availability of distributed systems. In International Working Conference on Component Deployment (pp. 99-114). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]
8. Kuhlenkamp, J., Klems, M., & Röss, O. (2014). Benchmarking scalability and elasticity of distributed database systems. Proceedings of the VLDB Endowment, 7(12), 1219-1230. [CrossRef]
9. Creel, K. A. (2020). Transparency in complex computational systems. Philosophy of Science, 87(4), 568-589. [CrossRef]

10. Ledmi, A., Bendjenna, H., & Hemam, S. M. (2018, October). Fault tolerance in distributed systems: A survey. In 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS) (pp. 1-5). IEEE. [CrossRef]
11. Nanthini, N., Vidhyasri, R., & Anand, V. V. (2024, April). Fault Tolerance Using AutoScaling in Amazon Web Services. In 2024 International Conference on Computing and Data Science (ICCDS) (pp. 1-6). IEEE. [CrossRef]
12. Ahmed, J., Karpenko, A., Tarasyuk, O., Gorbenko, A., & Sheikh-Akbari, A. (2023). Consistency issue and related trade-offs in distributed replicated systems and databases: a review. [CrossRef]
13. Hogade, N., Pasricha, S., & Siegel, H. J. (2021). Energy and network aware workload management for geographically distributed data centers. IEEE Transactions on Sustainable Computing, 7(2), 400-413. [CrossRef]
14. Lee, E. A., Bateni, S., Lin, S., Lohstroh, M., & Menard, C. (2021). Quantifying and generalizing the CAP theorem. arXiv preprint arXiv:2109.07771. [CrossRef]
15. Skorykh, O. (2022). Migration of NoSQL (Cassandra) to relational database (Postgres) on high demanded distributed system (Doctoral dissertation, Hochschule für Angewandte Wissenschaften Hamburg). [CrossRef]
16. Adoni, H. W. Y., Nahhal, T., Krichen, M., Aghezzaf, B., & Elbyed, A. (2020). A survey of current challenges in partitioning and processing of graph-structured data in parallel and distributed systems. Distributed and Parallel Databases, 38, 495-530. [CrossRef]
17. Brewer, E. A. (2000, July). Towards robust distributed systems. In PODC (Vol. 7, No. 10.1145, pp. 343-477). [CrossRef]
18. Khoshaba, O., Grechaninov, V., Molodetska, T., Lopushanskyi, A., & Zavertailo, K. (2022, November). Study of the Workspace Model in Distributed Structures Using CAP Theorem. In International scientific-practical conference (pp. 229-242). Cham: Springer Nature Switzerland. [CrossRef]
19. Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access, 9, 13938-13959. [CrossRef]
20. Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2020, October). Dynamic access control and authorization system based on zero-trust architecture. In Proceedings of the 2020 1st international conference on control, robotics and intelligent system (pp. 123-127). [CrossRef]
21. Daswani, N., Elbayadi, M., Daswani, N., & Elbayadi, M. (2021). The Equifax Breach. Big Breaches: Cybersecurity Lessons for Everyone, 75-95. [CrossRef]
22. Huang, H., Lin, J., Zheng, B., Zheng, Z., & Bian, J. (2020). When blockchain meets distributed file systems: An overview, challenges, and open issues. IEEE Access, 8, 50574-50586. [CrossRef]
23. B. Rawat, D., Chaudhary, V., & Doku, R. (2020). Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems. Journal of Cybersecurity and Privacy, 1(1), 4-18. [CrossRef]
24. Panwar, A., & Bhatnagar, V. (2020, February). Distributed ledger technology (DLT): The beginning of a technological revolution for blockchain. In 2nd International Conference on Data, Engineering and Applications (IDEA) (pp. 1-5). IEEE. [CrossRef]
25. Zhou, S., Li, K., Xiao, L., Cai, J., Liang, W., & Castiglione, A. (2023). A systematic review of consensus mechanisms in blockchain. Mathematics, 11(10), 2248. [CrossRef]
26. Esmat, A., de Vos, M., Ghiassi-Farrokhfal, Y., Palensky, P., & Epema, D. (2021). A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. Applied Energy, 282, 116123. [CrossRef]
27. Cherupally, S. R., Boga, S., Podili, P., & Kataoka, K. (2021, January). Lightweight and Scalable DAG based distributed ledger for verifying IoT data integrity. In 2021 International Conference on Information Networking (ICOIN) (pp. 267-272). IEEE. [CrossRef]
28. Zhao, W. (2021). From traditional fault tolerance to blockchain. John Wiley & Sons. [CrossRef]
29. Tikhomirov, S., Moreno-Sanchez, P., & Maffei, M. (2020, September). A quantitative analysis of security, anonymity and scalability for the lightning network. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 387-396). IEEE. [CrossRef]
30. Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. Sensors, 22(14), 5274. [CrossRef]
31. Mueller-Bloch, C., Andersen, J. V., Spasovski, J., & Hahn, J. (2024). Understanding decentralization of decision-making power in proof-of-stake blockchains: an agent-based simulation approach. European journal of information systems, 33(3), 267-286. [CrossRef]
32. Singh, A., Kumar, G., Saha, R., Conti, M., Alazab, M., & Thomas, R. (2022). A survey and taxonomy of consensus protocols for blockchains. Journal of Systems Architecture, 127, 102503. [CrossRef]
33. Cornito, C. M. (2021). Striking a Balance between Centralized and Decentralized Decision Making: A School-Based Management Practice for Optimum Performance. International Journal on Social and Education Sciences, 3(4), 656-669. [CrossRef]

34. Truong, N., Lee, G. M., Sun, K., Guitton, F., & Guo, Y. (2021). A blockchain-based trust system for decentralised applications: When trustless needs trust. Future Generation Computer Systems, 124, 68-79. [CrossRef]
35. Dong, J., Song, C., Liu, S., Yin, H., Zheng, H., & Li, Y. (2022). Decentralized peer-to-peer energy trading strategy in energy blockchain environment: A game-theoretic approach. Applied Energy, 325, 119852. [CrossRef]
36. Zhang, J., & Wu, M. (2021). Cooperation mechanism in blockchain by evolutionary game theory. Complexity, 2021(1), 1258730. [CrossRef]
37. Kiayias, A., & Zindros, D. (2020). Proof-of-work sidechains. In Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23 (pp. 21-34). Springer International Publishing. [CrossRef]
38. Saleh, F. (2021). Blockchain without waste: Proof-of-stake. The Review of financial studies, 34(3), 1156-1190. [CrossRef]
39. Saad, S. M. S., & Radzi, R. Z. R. M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). International Journal of Innovative Computing, 10(2). [CrossRef]
40. Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K. K. R. (2021). The application of the blockchain technology in voting systems: A review. ACM Computing Surveys (CSUR), 54(3), 1-28. [CrossRef]
41. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications, 14, 2901-2925. [CrossRef]
42. El Faqir, Y., Arroyo, J., & Hassan, S. (2020, August). An overview of decentralized autonomous organizations on the blockchain. In Proceedings of the 16th international symposium on open collaboration (pp. 1-8). [CrossRef]
43. Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry, 12(8), 1328. [CrossRef]
44. Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—review and open research challenges. Sensors, 21(17), 5874. [CrossRef]
45. Aufiero, S., Ibba, G., Bartolucci, S., Destefanis, G., Neykova, R., & Ortu, M. (2024). Dapps ecosystems: Mapping the network structure of smart contract interactions. arXiv preprint arXiv:2401.01991. [CrossRef]
46. Vacca, A., Di Sorbo, A., Visaggio, C. A., & Canfora, G. (2021). A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. Journal of Systems and Software, 174, 110891. [CrossRef]
47. Hauck, R. (2021). Blockchain, smart contracts and intellectual property. Using distributed ledger technology to protect, license and enforce intellectual property rights. Legal Issues in the Digital Age, 1(1), 17-41. [CrossRef]
48. Carvalho, A. (2021). Bringing transparency and trustworthiness to loot boxes with blockchain and smart contracts. Decision Support Systems, 144, 113508. [CrossRef]
49. Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. Electronics, 9(1), 94. [CrossRef]
50. Sookhak, M., Jabbarpour, M. R., Safa, N. S., & Yu, F. R. (2021). Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. Journal of Network and Computer Applications, 178, 102950. [CrossRef]
51. Appel, I., & Grennan, J. (2023, May). Control of decentralized autonomous organizations. In AEA Papers and Proceedings (Vol. 113, pp. 182-185). 2014 Broadway, Suite 305, Nashville, TN 37203: American Economic Association. [CrossRef]
52. Liu, L., Zhou, S., Huang, H., & Zheng, Z. (2021). From technology to society: An overview of blockchain-based DAO. IEEE Open Journal of the Computer Society, 2, 204-215. [CrossRef]
53. Bellavitis, C., Fisch, C., & Momtaz, P. P. (2023). The rise of decentralized autonomous organizations (DAOs): a first empirical glimpse. Venture Capital, 25(2), 187-203. [CrossRef]
54. Liang, X., Lin, Y., Fu, H., Zhu, L., & Li, X. (2022). Rscfed: Random sampling consensus federated semi-supervised learning. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 10154-10163). [CrossRef]
55. Hou, D., Zhang, J., Man, K. L., Ma, J., & Peng, Z. (2021, May). A systematic literature review of blockchain-based federated learning: Architectures, applications and issues. In 2021 2nd Information communication technologies conference (ICTC) (pp. 302-307). IEEE. [CrossRef]
56. De Filippi, P., & Lavayssière, X. (2020). Blockchain technology: Toward a decentralized governance of digital platforms?. The Great Awakening: New Modes of Life amidst Capitalist Ruins, 185-222. [CrossRef]
57. Zwitter, A., & Hazenberg, J. (2020). Decentralized network governance: blockchain technology and the future of regulation. Frontiers in Blockchain, 3, 12. [CrossRef]

58. Singh, S., Wable, S., & Kharose, P. (2021). A review of e-Voting system based on blockchain technology. International Journal of New Practices in Management and Engineering, 10(04), 09-13. [CrossRef]
59. Patel, R., Migliavacca, M., & Oriani, M. E. (2022). Blockchain in banking and finance: A bibliometric review. Research in International Business and Finance, 62, 101718. [CrossRef]
60. Ullah, N., Al-Rahmi, W. M., Alfarraj, O., Alalwan, N., Alzahrani, A. I., Ramayah, T., & Kumar, V. (2022). Hybridizing cost saving with trust for blockchain technology adoption by financial institutions. Telematics and Informatics Reports, 6, 100008. [CrossRef]
61. Tsao, Y. C., & Vu, T. L. (2022). A decentralized microgrid considering blockchain adoption and credit risk. Journal of the Operational Research Society, 73(9), 2116-2128. [CrossRef]
62. Dashkevich, N., Counsell, S., & Destefanis, G. (2020). Blockchain application for central banks: A systematic mapping study. IEEE Access, 8, 139918-139952. [CrossRef]
63. Queiroz, M. M., Telles, R., & Bonilla, S. H. (2020). Blockchain and supply chain management integration: a systematic review of the literature. Supply chain management: An international journal, 25(2), 241-254. [CrossRef]
64. Moosavi, J., Naeni, L. M., Fathollahi-Fard, A. M., & Fiore, U. (2021). Blockchain in supply chain management: a review, bibliometric, and network analysis. Environmental Science and Pollution Research, 1-15. [CrossRef]
65. Sunny, J., Undralla, N., & Pillai, V. M. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. Computers & Industrial Engineering, 150, 106895. [CrossRef]
66. Bader, L., Pennekamp, J., Matzutt, R., Hedderich, D., Kowalski, M., Lücken, V., & Wehrle, K. (2021). Blockchain-based privacy preservation for supply chains supporting lightweight multi-hop information accountability. Information Processing & Management, 58(3), 102529. [CrossRef]
67. Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks, 2, 130-139. [CrossRef]
68. Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 15(1), 70-83. [CrossRef]
69. Mann, S. P., Savulescu, J., Ravaud, P., & Benchoufi, M. (2021). Blockchain, consent and prosent for medical research. Journal of medical ethics, 47(4), 244-250. [CrossRef]
70. Odeh, A., Keshta, I., & Al-Haija, Q. A. (2022). Analysis of blockchain in the healthcare sector: application and issues. Symmetry, 14(9), 1760. [CrossRef]
71. Datta, A. (2021). Blockchain enabled digital government and public sector services: A survey. Blockchain and the Public Sector: Theories, Reforms, and Case Studies, 175-195. [CrossRef]
72. Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernández-Gutiérrez, M. (2021). Blockchain for public services: A systematic literature review. IEEE Access, 9, 13904-13921. [CrossRef]
73. Soner, S., Litoriya, R., & Pandey, P. (2021). Exploring blockchain and smart contract technology for reliable and secure land registration and record management. Wireless Personal Communications, 121(4), 2495-2509. [CrossRef]
74. Wang, Q., & Su, M. (2020). Integrating blockchain technology into the energy sector—from theory of blockchain to research and application of energy blockchain. Computer Science Review, 37, 100275. [CrossRef]
75. Kumar, N. M., Chand, A. A., Malvoni, M., Prasad, K. A., Mamun, K. A., Islam, F. R., & Chopra, S. S. (2020). Distributed energy resources and the application of AI, IoT, and blockchain in smart grids. Energies, 13(21), 5739. [CrossRef]
76. Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2021). Cybersecurity in next generation energy grids: Challenges and opportunities for blockchain and Ai technologies. Digital Transformation, Cyber Security and Resilience of Modern Societies, 299-314. [CrossRef]
77. Rane, S. B., & Narvel, Y. A. M. (2022). Data-driven decision making with Blockchain-IoT integrated architecture: a project resource management agility perspective of industry 4.0. International Journal of System Assurance Engineering and Management, 13(2), 1005-1023. [CrossRef]
78. Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., ... & Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. Future Generation Computer Systems, 131, 209-226. [CrossRef]
79. Theodorakopoulos, L., Theodoropoulou, A., & Stamatiou, Y. (2024). A State-of-the-Art Review in Big Data Management Engineering: Real-Life Case Studies, Challenges, and Future Research Directions. Eng, 5(3), 1266-1297. [CrossRef]
80. Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., ... & Tsolis, D. (2023). Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy, 3(3), 493-543. [CrossRef]
81. Rahim, R., Patan, R., Manikandan, R., & Kumar, S. R. (2020). Introduction to blockchain and big data. In Blockchain, Big Data and Machine Learning (pp. 1-23). CRC Press. [CrossRef]

82. Sundarakani, B., Ajaykumar, A., & Gunasekaran, A. (2021). Big data driven supply chain design and applications for blockchain: An action research using case study approach. Omega, 102, 102452. [CrossRef]
83. Bhuiyan, M. Z. A., Zaman, A., Wang, T., Wang, G., Tao, H., & Hassan, M. M. (2018, May). Blockchain and big data to transform the healthcare. In Proceedings of the international conference on data processing and applications (pp. 62-68). [CrossRef]
84. Li, J., Herdem, M. S., Nathwani, J., & Wen, J. Z. (2023). Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management. Energy and AI, 11, 100208. [CrossRef]
85. Antonopoulou, H., Theodorakopoulos, L., Halkiopoulos, C., & Mamalougkou, V. (2023). Utilizing machine learning to reassess the predictability of bank stocks. Emerging Science Journal, 7(3), 724-732. [CrossRef]
86. Kuo, T. T., & Ohno-Machado, L. (2018). Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. arXiv preprint arXiv:1802.01746. [CrossRef]
87. Rubio, M. A., Tarazona, G. M., & Contreras, L. (2018). Big data and blockchain basis for operating a new archetype of supply chain. In Data Mining and Big Data: Third International Conference, DMBD 2018, Shanghai, China, June 17–22, 2018, Proceedings 3 (pp. 659-669). Springer International Publishing. [CrossRef]
88. Paramesha, M., Rane, N., & Rane, J. (2024). Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence. Available at SSRN 4855856. [CrossRef]
89. Karafiloski, E., & Mishev, A. (2017, July). Blockchain solutions for big data challenges: A literature review. In IEEE EUROCON 2017-17th International Conference on Smart Technologies (pp. 763-768). IEEE. [CrossRef]
90. Guo, L., Xie, H., & Li, Y. (2020). Data encryption based blockchain and privacy preserving mechanisms towards big data. Journal of Visual Communication and Image Representation, 70, 102741. [CrossRef]
91. Karras, A., Giannaros, A., Theodorakopoulos, L., Krimpas, G. A., Kalogeratos, G., Karras, C., & Sioutas, S. (2023). FLIBD: A federated learning-based IoT big data management approach for privacy-preserving over Apache Spark with FATE. Electronics, 12(22), 4633. [CrossRef]
92. Wibowo, S., & Sandikapura, T. (2019, November). Improving data security, interoperability, and veracity using blockchain for one data governance, case study of local tax big data. In 2019 International Conference on ICT for Smart Society (ICISS) (Vol. 7, pp. 1-6). IEEE. [CrossRef]
93. Ahsan, A., & Shabbir, A. (2021). Blockchain and Big Data: Exploring Convergence for Privacy, Security and Accountability. Sage Science Review of Educational Technology, 4(2), 53-68. [CrossRef]
94. Alza Jr, G. (2021). Blockchain & CCPA. Santa Clara High Tech. LJ, 37, 231. [CrossRef]
95. Xu, C., Wang, K., Li, P., Guo, S., Luo, J., Ye, B., & Guo, M. (2018). Making big data open in edges: A resource-efficient blockchain-based approach. IEEE Transactions on Parallel and Distributed Systems, 30(4), 870-882. [CrossRef]
96. Fahlevi, M., Moeljadi, M., Aisjah, S., & Djazuli, A. (2023). Corporate Governance in the Digital Age: A Comprehensive Review of Blockchain, AI, and Big Data Impacts, Opportunities, and Challenges. In E3S Web of Conferences (Vol. 448, p. 02056). EDP Sciences. [CrossRef]