applied sciences

MDPI

*Review*

# Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey

**Sumaira Johar [1,*], Naveed Ahmad [1], Warda Asher [1], Haitham Cruickshank [2] and Amad Durrani [1]**

[1] Department of Computer Science, University of Peshawar, Peshawar 25000, Pakistan;
n.ahmad@uop.edu.pk (N.A.); syeda.warda1406@gmail.com (W.A.); amad.durrani@uop.edu.pk (A.D.)
[2] Institute of Communication Systems, University of Surrey, Guildford GU2 7JP, UK;
H.Cruickshank@surrey.ac.uk
* Correspondence: sumaira.johar@uop.edu.pk

**Abstract:** Blockchain being a leading technology in the 21st century is revolutionizing each sector of life. Services are being provided and upgraded using its salient features and fruitful characteristics. Businesses are being enhanced by using this technology. Countries are shifting towards digital currencies i.e., an initial application of blockchain application. It omits the need of central authority by its distributed ledger functionality. This distributed ledger is achieved by using a consensus mechanism in blockchain. A consensus algorithm plays a core role in the implementation of blockchain. Any application implementing blockchain uses consensus algorithms to achieve its desired task. In this paper, we focus on provisioning of a comparative analysis of blockchain's consensus algorithms with respect to the type of application. Furthermore, we discuss the development platforms as well as technologies of blockchain. The aim of the paper is to provide knowledge from basic to extensive from blockchain architecture to consensus methods, from applications to development platform, from challenges and issues to blockchain research gaps in various areas.

**Keywords:** blockchain; applications; consensus mechanisms

check for updates

**Citation:** Johar, S.; Ahmad, N.; Asher, W.; Cruickshank, H.; Durrani, A. Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey. *Appl. Sci.* **2021**, *11*, 6252. https://doi.org/10.3390/app11146252

Academic Editor: Gianluca Lax

Received: 8 May 2021
Accepted: 26 June 2021
Published: 6 July 2021

## 1. Introduction

The 21st century is all about revolutionizing technology. One of the leading technologies that has changed many aspects is blockchain. It impacted different businesses from the very first step. Blockchain provides decentralized, transparent and secure systems. It is a distributed ledger technology which maintains a transaction ledger and secures it by using cryptography. The transactions are recorded in blocks and these blocks are connected to each other through hashes. Initially it was used by Satoshi Nakamoto in 2008 for public transactions of bitcoins. Bitcoin [1] digital currency was the first application of blockchain [2,3].

Blockchain came as a solution to the longstanding user's trust problem. With its emergence with the renowned cryptocurrency Bitcoin, it provided an architecture to allow the user to trust a decentralized system instead of trusting a third party. Operating a peer-to-peer network, it keeps records of the ledger of transactions. This helps to avoid any center party. The whole process is done through a consensus. A ledger is shared between multiple entities, allowing everyone to inspect it. No single user can control it. It is a distributed cryptographically secured database that keeps the record of every transaction from the very initial one.

### 1.1. Main Features of Blockchain

The following are the main features of blockchain.

1. Decentralized Computation: Blockchain consists of distributed ledgers maintained by peer to peer networks [4]. Blockchain eliminates the role of the central entity by using consensus protocol to validate transactions [5].

2. Distributed Ledger of Transactions: A shared ledger is used to store transactions [6,7]. A copy of the ledger is maintained on every peer of the blockchain network. These copies are synchronized by timely replication [8].
3. Transparency: Blockchain stores every transaction in a block. Also, it is available to all the peers for verification [9].
4. Security: Each block is added to the chain after validation. Also, each block contains a hash of the previous block [10]. It is computationally impossible to delete or update a block because it requires re-calculation of all the preceding block hashes.
5. Fault Tolerant Network: Blockchain has a peer-to-peer network of nodes. All miner nodes process transactions in parallel [11]. The blockchain will continue working if some of the nodes fail to function.

### *1.2. Working Flow of Blockchain*

The information in a blockchain is stored in cryptographically encrypted chunks known as blocks [12]. The next successive block contains information about the previous block and hence forms a chain. Thereby it gets its name. Each block in a blockchain contains a unique hash, transaction data and hash of the previous block. The initial block is known as genesis block. A genesis block does not contain a previous hash. Participants of the blockchain network can be organizations, individuals or institutions which share a copy of the ledger that contains their valid transactions in a sequential manner [13]. The new transactions are added to the existing records by consensus of the miners participating in that network. To validate the transactions, miners have to implement the blockchain's algorithm in order to be rewarded with a native token as per existing economic consensus mechanisms like proof of work, proof of stake, etc.

The fastest miner validate each transaction in a block and add it to the blockchain. In bitcoin, miner nodes take approximately 10 minutes to validate and add to the blockchain. A miner is selected from a pool of miners using a proof-of-work (PoW) consensus mechanism [14]. A blockchain uses a consensus mechanism to allow the miners to agree on a single value. After successful validation by all the miners in the blockchain network, the block is added to the blockchain. The miner obtains a transaction fee and new block addition fee in case of PoW [15]. The ledger runs on a peer to peer network and thus all the nodes participating in the network get a copy of the original information.

### *1.3. Key Characteristics*

As based on a peer-to-peer network. If any node's information in a blockchain is tampered with, it will not match the information copied on other nodes. As a result, the tampered copy will get discarded as the majority will not agree on the tampered copy to be true. Hence, any third party or broker is discarded by building secured trusted peer to peer network and based on rules implemented by consensus mechanisms.

A blockchain network has the following key characteristics:

- Consensus: All participants must agree on validity of a transaction for it to be valid. Blockchain offer a variety of consensus algorithms which are chosen by the users according to the requirement of blockchain application.
- Provenance: Participants know where the asset came from and how its ownership has changed over time.
- Immutability: No participant can tamper with a transaction after it has been recorded to the ledger [16,17]. If there is an error in a transaction, a new transaction must be used to reverse the error. Both these transactions are then visible [18]. The error in transaction means that the transactions are either failed or rejected by miners. Usually the transactions with very low fee are rejected.
- Finality: A single, shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.
- Smart Contract: The smart contracts [19] are programs of computer that support in the transmission of money or anything of value. When a particular policy is met,

these programs run automatically. Each smart contract contains a contract address, predefined functions and private storage. Ethereum [20], is an open-source and decentralized platform that executes smart contracts. To construct smart contract Ethereum platform uses solidity as programming language.

### 1.4. Research Questions

The following are the research questions are answered in this survey article.

- How can blockchain can be deployed in different applications?
- What are the potential consensus methods for public and private blockchains?
- Which platforms offer development of blockchain?
- What are potential attacks for blockchain and what are the research issues in different applications of blockchain?

### 1.5. Research Contributions

Some of the major contributions of the paper are as follows.

- The core blockchain is discussed i.e., its architecture, its working flow and characteristics.
- The paper also discusses different applications of blockchain.
- This paper focuses on the survey of the consensus algorithms of the public and private blockchains.
- The algorithms are categorized according to their use in different scenarios and fields.
- The survey papers are compared in Tables 1 and 2 also as a major contribution of our paper.

### 1.6. Organization

Further the paper is divided as follows. Section 2 discusses blockchain types. Section 3 explains different applications of blockchain other than cryptocurrencies. Section 4 discusses blockchain's architecture. In Section 5 we describe various consensus algorithms. Section 6 contains detailed discussion on blockchain development platforms. Section 7 contains blockchain challenges where possible attacks are discussed. Section 8 highlights some of the blockchain research issues in different areas. In Section 9, we present the conclusion and future work.

**Table 1.** Comparison of survey articles.

| Articles | Blockchain Applications | Blockchain Architecture | Development Platform | Crypto Currencies | Health Care | Intelligent Transport Systems and Vehicular Adhoc Networks | Supply Chain | Internet of Things | Big Data | Cellular Networks | Social Networks | Distributed Web Services and Storage | Governance | Entertainment | Real Estate | Power | General |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Comparative Analysis of Consensus Algorithms [21] | No | No | No | Yes | No | No | No | No | No | No | No | No | No | No | No | No | No |
| State of the Art and Challenges Facing Consensus Protocols on Blockchain [22] | No | No | No | Yes | No | No | No | No | No | No | No | No | No | No | No | No | Yes |
| A survey on Consensus Mechanisms and Mining Management in Blockchain Networks [23] | Yes | Yes | No | Yes | Yes | Yes | No | Yes | No | Yes | No | No | No | No | No | No | Yes |
| A survey about consensus algorithms used in blockchain [24] | No | Yes | No | Yes | No | No | No | No | No | No | No | No | No | No | No | No | No |
| Proposed work | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

**Table 2.** Existing surveys vs. Proposed survey.

| Existing Surveys | Proposed Survey |
|---|---|
| Applications of blockchain other than cryptocurrencies are rarely discussed [21,22]. | About 14 blockchain applications covered. |
| Blockchain architecture rarely discussed [21,22]. | Blockchain architecture covered. |
| Consensus algorithms used in cryptocurrencies discussed are few in number [21–24]. | Discusses a large number of consensus algorithms used in cryptocurrencies as well as of other applications. |
| Development platforms are not discussed [21,23,25]. | Development platforms are discussed. |
| Existing surveys related to consensus algorithms of blockchain can be read for the understanding of consensus based on a particular application [21–25]. | This paper gives a broader view of different blockchain applications and the consensus used in those applications, making it easy for the researchers to follow the same consensus for a specific application. However one can also compare the consensus for the optimized solution of their work. |

## 2. Types of Blockchain

There are three main types of blockchain. These do not often confuse traditional databases or distributed ledger technology (DLT) with blockchains. These types of blockchain are:

1. Public/Permissionless Blockchains for example Bitcoin and Ethereum etc.
2. Private/Permissioned Blockchains for example Hyperledger and R3 Corda etc.
3. Hybrid Blockchains for example Dragonchain etc.

### *2.1. Public/Permissionless Blockchains*

Blockchain that has no restriction on accommodating anonymous participants is known as permissionless blockchain [26]. The term public blockchain is used interchangeably. Lottery based consensus algorithms are used to publish a block. A single node is responsible for publishing a block. Lottery-based mechanisms elect the validator to decide the next block to be added into the blockchain ledger. Election is based on a lottery draw and the one who wins is the validator. Each new block is appended using a new draw. The lottery-based mechanism avoids the malicious node having forged block to append it into the ledger. Such mechanisms do not follow a rule of thumb for electing the validator hence each lottery has its own trust model for electing the validator. If voting based consensus is allowed to be used in permissionless blockchain, multiple accounts can be made by the participants to do a Sybil attack to make the decisions in their favour. A sybil attack is one of the issue in peer to peer network where a malicious node creates many identities and tries to manipulate the network by controlling it. Public blockchains need security and for this purpose the block creation mechanism needs to be difficult and expensive so that the resources of one node are not enough to bias the decisions in its favor. The disadvantage of public blockchain is in terms of PoW where heavy computation power is needed. All the nodes need to solve a cryptographic puzzle by brute force. The node which wins the puzzle is rewarded and all the other nodes computations are wasted. The consensus is achieved as 51% of power. Proof of stake uses the wealth of miners to win a ticket rather than computational power [27]. There are other various consensus algorithms for private and public blockchains which are discussed in Section 5.

### *2.2. Private/Permissioned Blockchains*

Private and consortium blockchains are permissioned blockchains. In such types of blockchain the number of participants are limited and they keep a copy of the blockchain [28]. Consensus mechanism is not much expensive for publishing a new block. All the participants in the permissioned blockchain are known so the risk of Sybil attack is eliminated. Private blockchains voting mechanisms for consensus are used. Hence, permissioned blockchains have higher performance than permissionless blockchains. Non-public blockchains are divided into fully private or consortium blockchains. An organization can choose one of them based on the cost and needs. A consortium can be the best option if organizations want to share cost and data.

### *2.3. Hybrid Blockchains*

A hybrid blockchain combines the privacy of a private blockchain with the security and transparency of a public blockchain [29,30]. This gives the businesses a significant amount of options to choose from for what they want to keep private and what to be made public. For example, Dragonchain blockchain is a hybrid blockchain [31]. It allows its users to connect with other blockchain protocols. Thus, allowing blockchains multichain network. This functionality makes it simple for businesses to operate with the transparency they are looking for, without having to sacrifice security and privacy. Being able to post to multiple public blockchains at once increases the security of transactions, as they benefit from the combined hash power being applied to the public chains [32]. A careful study of the system is needed before implementing blockchain in any industry or business. The following are to be considered for the deployment of blockchains.

- Does business deals through trusted third parties?
- Do people frequently generate transactions?
- Are validation and data integrity important?
- Is the data integrity and process performance more important than confidentiality? However for time sensitive nature of the application it is not recommended as the transactions take time to be validated and verified.
- Blockchain can influence several emerging areas like smart cities, Internet of Vehicles, banking, Internet of Things, edge computing and cloud [33].
- Is blockchain required to be deployed as public or private?

## 3. Applications of Blockchain

Blockchain has now being deployed in not only cryptocurrency but its underlying technology is used in various applications [34]. We tried to discuss a few applications of blockchain which includes cryptocurrencies as well as other potential areas where blockchain has emerged. Figure 1 shows different applications of blockchain. However the applications are not limited to the ones discussed in this paper.

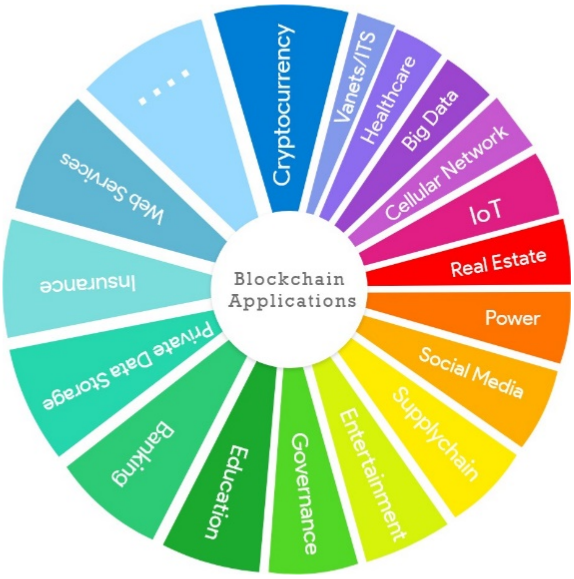

**Figure 1.** Applications of blockchain.

### 3.1. Cryptocurrency

Over the past decade cryptocurrency is being an evolving topic, merging incredible technical power and enticing investments worth of value trillions dollars on a world wide scale. The underlying technology of cryptocurrency is attractive for many other applications due to its unique features and architecture. This is why it is becoming popular due to its applicability, efficiency and data-centric characteristics [35]. Cryptocurrencies such as bitcoin use blockchain technology to secure transactions using hashes. Bitcoin was the first cryptocurrency using blockchain with Proof of Work algorithm.

### 3.2. Private Data Storage

The transactions are used to carry instructions for queuing, storing and sharing data. As the increased number of mobile applications needs access to complete access of user data that is: contacts, photos, messages and other important user data. Zyskind et al. proposed the blockchain implementation with other offline storage methods to provide permissions on each set of data. LevelDB [36] or cloud storage can be used to bound the data on blockchain. This could lead to dependency on third parties but provides more scalable solutions. Companies can go for upgrading technology finding more reliable solution for the data that need privacy solutions.

### 3.3. Reputation Management

Private blockchain can be implemented for direct and real time feedback from participants without intermediaries to help in auditing and invoicing or any other value of reputation. By the use of this technology, manual collection and transmission of feedback has been reduced. This type of blockchain can be retrieved by the participants in case they want to know the reputation of other participants [37,38].

### 3.4. Education

Sharples and Dommingue [39] suggested the use of blockchain to keep educational records and rewards. They also suggested the use of an educational reputation currency to be given as reward. Ref. [40] described how the founder of education use blockchain for online courses can. This technology can record the student signed up for the course and verify that the student has completed and learned the course. A payment feature can be added for the use of smart contracts by students to ensure lifelong learning plans [41]. Mega University is an example of technology being used by the students to establish their own ways of learning and access the faculty for collaborative experiences. A higher education credit and grading systems is suggested in [42] which is a consolidated outlook for higher education institutions and students.

### 3.5. Banking

Blockchain can be useful in computerization of various niche aspects of banking like, data loss reporting, client account reconciliations, clearing settlement and over the contracts (OTC) contracts/products etc. Classic banking methods like endorsement of a loan or derivative is a time taking process due to several back end stages which involves contract consultations with multiple parties. Blockchain provides the essential transparency and speed through smart contracts. Various banks are already testing blockchain and they are obtaining services from technology companies such as IBM, R3 and Microsoft.

### 3.6. Finance-Payroll and Settlement

Public service transactions involve a sequence of activities to legalize the validity of the transacting party, authentication of the data delivered by the transacting party or parties, performing of the transaction and finally delivery of the compulsory service. The transactions are then recorded from end to end. This process take a long time. The blockchain can reduce this time because of it nature of validity and authenticity. Since a large number of events connected to life built pension such as getting expenses from active customers, beneficiaries obtaining their payments and taxes on pensions are basically contract controlled payments. Sestoft [43] has suggested the use of Ethereum as the algorithm should work on self-regulated contracts. A prerequisite here is the fact that such an autonomous system will need event insurance relates life event triggers from other trusted bodies, so that self-executing contracts can act on them.

Sesoft proposed a distributed system for an Autonomous Pension Fund which is a contract based system which would manage life based pension funds without any intermediary.

### 3.7. Taxation

Blockchain can help in the collection of taxes from end to end and expenditure of taxes by the government. Taxation is one area where blockchain can possibly make a big impact. The key terms of blockchain, transparency, provenance and traceability can be related to the needs of taxation systems. Blockchain can be applied to tax transactions, VAT, stamp duties and withholding tax etc. Shifting taxation cab remove the responsibility of tax authorities where they collect taxes. While the tax provenance aspect is very important so also is the consumption of tax incomes. The biggest issue, however, would be to digitize the non-digital sellers who reply mostly on paper records.

### *3.8. Healthcare*

Healthcare is moving towards digitization with an increased number of hospitals, doctors, healthcare machinery to record patient's record digitally [44]. Digitization of medical data allows sharing and retrieval easily for decision making purposes. However such digitization is risky in terms of patient privacy violation. A blockchain-based Healthcare Data Gateway (HDG) was proposed by Yue et al. [45]. They used a private blockchain cloud to guarantee that the medical data cannot be changed by anybody including the patient himself and/or the physicians. A blockchain-based interoperable Electronic Health Record (EHR) framework proposed by [46] provides important reliability and security requirements. It enables different organizations of variant internal structures to communicate with each other using the existing EHR infrastructure of organizations.

Reference [25] has also proposed MeDShare, a blockchain based system for distribution of medical data between cloud service providers. MeDShare would provide auditing, data access control and provenance. Blocking of malicious users and the use of smart contracts for data behavior recognition from data access patterns, is also proposed in same work. Medchain presented in [47] suggests an efficient data sharing system via blockchain.

### *3.9. Voting*

In the year 2014, a Danish political party was the first to use blockchain technology for voting [48]. 'Followmyvote' offers an online voting platform which follows blockchain technology for secure voting system [49].

A challenge for fair voting system which keeps users' voting privacy and that provides transparency and flexibility of electronic system is solved in this paper. A novel blockchain application for fair electronic voting is proposed by [50] which eliminates some of the existing systems issues. It particularly addresses the election process which reduces the cost of conducting elections nationwide.

### *3.10. Insurance*

With the use of blockchain, travel insurance, crop insurance, property and casualty insurance and most importantly health insurance are all going to change [51]. A shared network of hospital insurance authorities, funeral houses and health departments can be created. This set up will provide non dependency on third parties speed up the whole process of claiming insurance, it can also eliminate frauds.

In Reference [52], blockchain is proposed to handle the transactions related to insurance process efficiently. They have used hyperledger fabric for the design implementation which is an open source permissioned blockchain platform.

### *3.11. Smart Cities*

In smart cities information and communication technologies are used to share resources. Blockchain is used in smart cities to reduce transaction costs, to achieve data immutability and accountability. The problem in [53] of data storage from sensors and its management is solved using blockchain technology. The blockchain answers to the request of accessibility and validity by offering smart contract facility where sensor information is managed and control logic is implemented.

### *3.12. Internet of Things (IOT)*

The Internet of Things (IoT) is a network of connected vehicles, home appliances, physical devices, and other items that are accessible through the Internet [54]. IoT is widely used in smart homes, smart grid, intelligent manufacturing, intelligent transportation system, and other fields [55,56]. The traditional centralized network does not guarantee trusted interaction among devices and security of sensitive information. Therefore, the combination of blockchain and IoT is an expected trend, where smart contracts will help to automate, promote resource sharing, complex workflow, ensure safety, efficiency and save costs [57]. A smart home model is proposed by Dorri et al. [58] which is based on blockchain and smart contracts. They discussed how through simulations the cost of daily management of IoT devices can be reduced. They also discussed in the model, various interaction processes.

### *3.13. Blockchain in Social Media*

Blockchain has played an important role in social media applications. The reason it is spreading is privacy. Being on blockchain takes away the concept of being centralized. Common examples are Ushare [59], DUST, BeeChat etc. Some of those applications provide anonymity which may give way to malicious behavior. We now discuss some of the top blockchain based social media networks as shown in Figure 2.

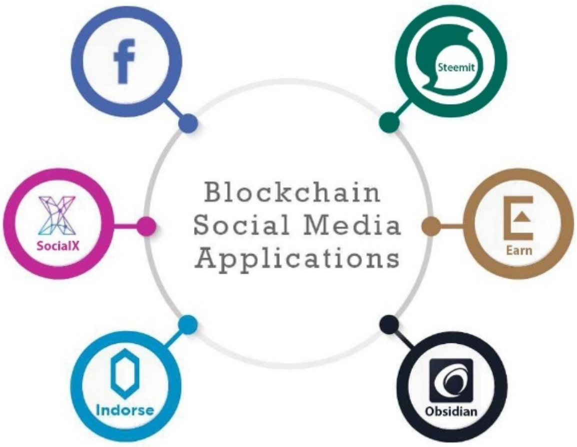

**Figure 2.** Blockchain in social media.

#### 3.13.1. Steemit

Steemit provides the services of both Redit and Facebook and so it is one of the top blockchain based social media apps. This platform allows users to post their pictures, posts, music and video and get paid for the content. This platform automatically distributes Steemit currency units to active users.

#### 3.13.2. Earn

Earn is better than LinkedIn. Earn allows users to earn by completing microtasks. Users need to create a profile and they receive paid messages or they would get an opportunity to join people with similar skills. The paid email system of Earn can increase the chances of making money.

#### 3.13.3. SocialX

SocialX is very much similar to Instagram and Facebook except that it's decentralized. This platform has all the social network features and it allows users to post pictures and videos on a highly secure platform. SocialX has a built-in license management which gives users the choice to sell their photos and videos or keep them to themselves.

#### 3.13.4. Obsidian

Obsidian provides a wide collection of blockchain based apps but the main service is secure messenger. This allows users to chat 100% privately and securely. Obsidian provides end to end encryption which proves the files and messages are seen only by the intended recipient.

#### 3.13.5. Indorse

Indorse is a professional platform based on the Ethereum blockchain. This is a LinkedIn equivalent which increases the chances for users to get profit for their skills. Users get paid or get impressive rewards for their contributions. For example if a user is good at coding he will be validated by experts or a user can get a good job by showing business skills.

### 3.14. Blockchain in Power

Another area of blockchain is to enable customers to quickly switch power suppliers. Companies are also using blockchain for meter registration to make the process less costly and more efficient. Blockchain may also make existing electric industry methods more efficient by helping the utilities' "smart grid" management systems that spontaneously diagnose network problems and emergencies and in reaction reconfigure the network [60].

## 4. Blockchain's Architecture

As discussed earlier, the initial block in a block chain is known as the genesis block. A genesis block does not contain a previous hash but its own hash. Figure 3 shows a general view of a blockchain. A block contains the transactions, hash of the previous block and hash of the next block [61]. This information is stored in a block using a cryptographic mechanism. A block in the chain can come from any miner. While creating the chain of blocks, the hash of the previous block is added to the current block. Thus a miner creates a new block by using the hash of the previous block, combines it with its own set of messages, and creates a new hash out of it. This way a new block is formed. This recently formed block now turn out to be the new end for the chain. By this mechanism the chain grows as more blocks are added by the miners.

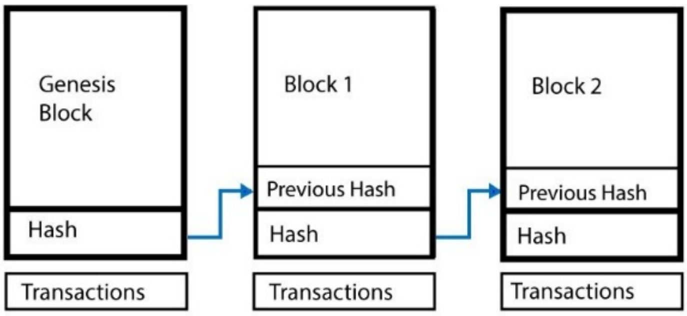

**Figure 3.** Blockchain architecture [62].

Double-spending is the problem where the sender uses the same money at more than one place for gaining goods or services from multiple dealers. The use of centralized authority solves the double-spending problem, but another main issue arises which is the cost of maintaining and creating the centralized authority itself. Blockchain however prevents double-spending by grouping the transactions and timestamping them and then broadcasting them in the network to all the participant nodes. The transactions are mathematically related to previous ones and are timestamped, hence impossible to tamper with.

There are also some other fields in the block header which are shown in Figure 4. We explain each of them.

### 4.1. Previous Hash

This field contains a hash of the previous block which connects the current block with its parent in the chain. A hash value is calculated from all the information of the previous block and this value is given to the field prev_hash which resides in the new block. This hash value is calculated from SHA 256 in bitcoin.

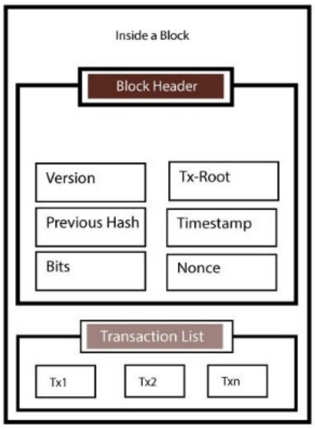

**Figure 4.** Structure of a block [23].

### *4.2. Timestamp*

This is the time when a new block is created [63].

### *4.3. Tx–Root*

This field is also known as the Merkle root, and it contains the hash value of the block which has all the validated transactions [64]. As shown in Figure 2, a hash value is calculated out of transactions where these transactions are combined pair by pair and are then combined for another hash function. These steps are repeated until they all are combined in a single entity called Merkle root.

### *4.4. Version*

This contains the version of protocol used by that particular node which proposes a block to the chain.

### *4.5. Nonce*

This field is used in PoW, which proves the efforts that a node has paid for getting the right to append his block to the chain. This field will be presented in the next section.

### *4.6. Bits*

This field represents the difficulty level of the PoW [65].

### *4.7. Transactions List*

A transaction in a broad sense is an exchange, agreement, understanding, contract, or transfer of cash/assets or property that happens between more than two parties and launches a legal compulsion. Transactions are recorded first in a journal and then dispatched to a ledger. A transaction is an interchange of goods or services between a seller and a buyer. Every transaction has three constituents: (1) transfer of service/good and money, (2) transfer of exchange privileges and (3) transfer of label which may or may not be complemented by a transfer of ownership. Blockchain transaction is a public record of all transactions that is executed on Blockchain. A block is the recent part of a blockchain which records the current information. Once a block is completed, it publishes into the blockchain as a lasting database creating a new block.

## **5. Consensus Algorithms**

We know that blockchain is a decentralized distributed network that provides security, immutability, transparency and privacy. There is no concept of centralization to verify and validate the transactions, but still transactions in the blockchain are considered to be completely verified and secured. This is the result of a core algorithm present in every blockchain network called a consensus protocol.

A consensus algorithm is a technique through which all the peers of the blockchain network reach a common agreement about the current state of the distributed ledger. Therefore, consensus algorithms provide trust and reliability among unknown peers in a distributed environment. A consensus mechanism ensures that every new block added to the blockchain is the only truth which is agreed upon by all the blockchain nodes [66].

The blockchain consensus protocol comprises some specific aims that are coming to an agreement, co-operation, collaboration, mandatory participation of each node in the consensus process and equal rights to every node. Hence, a consensus algorithm targets at finding a common agreement that is a win for the whole network. The above discussed applications are categorized and consensus algorithms based on these categories are further discussed below. Figure 5 shows a categorical diagram of the consensus and their distribution.

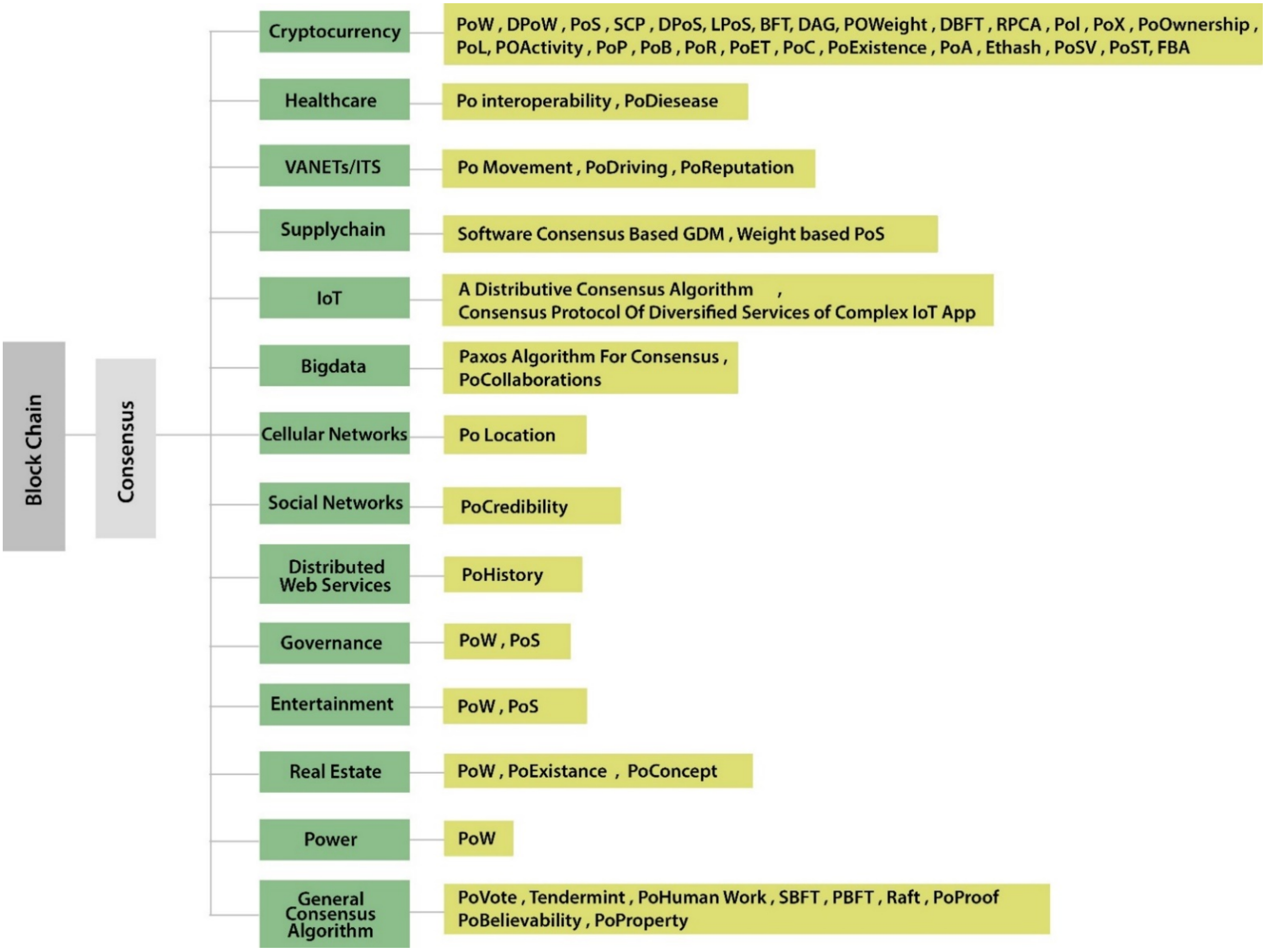
Block Chain
Consensus
Cryptocurrency
PoW , DPoW , PoS , SCP , DPoS, LPoS, BFT, DAG, POWeight , DBFT , RPCA , PoI , PoX , PoOwnership , PoL, POActivity , PoP , PoB , PoR , PoET , PoC , PoExistence , PoA , Ethash , PoSV , PoST, FBA
Healthcare
Po interoperability , PoDiesease
VANETs/ITS
Po Movement , PoDriving , PoReputation
Supplychain
Software Consensus Based GDM , Weight based PoS
IoT
A Distributive Consensus Algorithm ,
Consensus Protocol Of Diversified Services of Complex IoT App
Bigdata
Paxos Algorithm For Consensus ,
PoCollaborations
Cellular Networks
Po Location
Social Networks
PoCredibility
Distributed Web Services
PoHistory
Governance
PoW , PoS
Entertainment
PoW , PoS
Real Estate
PoW , PoExistance , PoConcept
Power
PoW
General Consensus Algorithm
PoVote , Tendermint , PoHuman Work , SBFT , PBFT , Raft , PoProof
PoBelievability , PoProperty

**Figure 5.** Categorization of the consensus algorithms.

### 5.1. Consensus Algorithms Used by Various Cryptocurrencies

Digital currencies have gained faster payment methods by using blockchain. Bitcoin was the first cryptocurrency used by blockchain. After gaining popularity in bitcoin other applications were/are implemented. Table 3 defines some of the important characteristics of consensus algorithms used in cryptocurrencies.

**Table 3.** Characteristics of cryptocurrency consensus algorithms.

| S.No | Consensus Algorithms | Permissioned/Permissionless | Platform | Programming Language | Advantages | Disadvantages |
|---|---|---|---|---|---|---|
| 1 | Proof of Work (PoW) [67] | Permissionless | Bitcoin | C++ | Better security, Suitable for variety of applications | Wastes considerable energy, 51% Attack possible Advance hardware required |
| 2 | Delayed Proof of Work (DPoW) [68] | Permissionless (But it can be customized as permissioned) | Komodo | Python | Energy efficient, Increased security | Blockchain using Pow and PoS can be part of this consensus |
| 3 | Proof of Stack (PoS) [21] | Permissionless | Peercoin.Nxt, Blackcoin, Shadow coin, Ethereum | Java | High speed Less energy consumption, No advance hardware required | Rich get richer |
| 4 | Steller Consensus Protocol (SCP) [20] | Permissionless | Steller | C/C++, JavaScript, Go etc. | Fast transactions with low fees | Inefficient in case of number of messages sent |
| 5 | Delegated Proof of Stack (DPoS) [69] | Permissioned/Permissionless | Steem.it, EOS, Bitshares, Lisk | Javascript, C++, Ark | Secure Real-time Voting, Better distribution of rewards | Cartel formation, Easier for 51% attack, Partially decentralized |
| 6 | Leased Proof of Stack (LPoS) [70] | Permissioned | Waves | Scala | Fair usage, lease coins | Decentralization issue |
| 7 | Byzantine Fault Tolerance (BFT) [71,72] | Permissionless | Ripple, Steller, Hyperledger Fabric | Not known | Less Energy consumption, No advance hardware, Fast, Scalable | Less suitable for public blockchain |
| 8 | Directed Acyclic Graph (DAG) [73] | Permissionless | Iota, Hashgraph, Byteball, Raiblocks/Nano | Javascript, Rust, Java, Go, C++ | Low-cost Network, Scalable | Difficult implementation, Not good for smart contracts |
| 9 | Proof of Weight [74] | Not Known | Filecoin, Algorand, Chia | Succinct Non-interactive Argument of Knowledge (SNARK)/Succinct Transparent Argument of Knowledge (STARK) | Scalable, Customizable | Incentivization issue |
| 10 | Delegated Byzantine Fault Tolerance (DBFT) [75] | Permissioned/Permissionless | Neo | C#, Python, .NET, Java, C++, C, Go, Kotlin, Javascript | Fast, scalable | Conflictions on the chain |

**Table 3.** *Cont.*

| S.No | Consensus Algorithms | Permissioned/Permissionless | Platform | Programming Language | Advantages | Disadvantages |
|---|---|---|---|---|---|---|
| 11 | Ripple Protocol Consensus Algorithm (RPCA) [20,76] | Permissionless | XRP | Java, C++, Node.js | Energy efficient, quick | Centralization |
| 12 | Proof of Importance (PoI) [75] | Permissionless | XEM | Java, C++ | Vesting Transaction partnership | Decentralization issue |
| 13 | Proof of Exercise (PoE) [20] | Permissionless | NA | NA | Avoid wastage of computational power | Needs dedicated research for practical implementation |
| 14 | Proof of Ownership (PoO) [75] | Permissionless | Decentalized credits (Decred) | Go | Use of unique pseudonyms makes multiple attacks difficult | Not known |
| 15 | Proof of Luck (PoL) [77] | Not Known | TEE (Trusted Execution Environment) such as Intel SGX-enabled CPUs | Not known | Decentralized, Low latency with transaction validation, Power safe | Prone to revision attack Forking, Unfair |
| 16 | Proof of Activity (PoA) [75] | Permissionless | Bitcoin or Bitcoin related technologies | Solidity, Java, Python | Equal contribution, Reduces 51% attack | Better energy consumption, Double signing |
| 17 | Proof of Publication (PoP) [21] | Permissioned | Bitcoin or Bitcoin related technologies and General Applications | Python, C++, Shell, Javascript | Can be used in cryptocurrency and general applications | No Energy saving |
| 18 | Proof of Burn (PoB) [21] | Permissionless | Slimcoin/Redcoin | Golang, C++, Solidity, LLL Serpent | Network preservation | Coins wastage, Not good for short term investors |
| 19 | Proof of Retrievability (PoR) [78] | Permissioned/Permissionless | Microsoft, Permacoin | Golang, C++, Solidity, LLL Serpent | Efficient | Extending the quantity of queries is challenging |

**Table 3.** *Cont.*

| S.No | Consensus Algorithms | Permissioned/Permissionless | Platform | Programming Language | Advantages | Disadvantages |
|---|---|---|---|---|---|---|
| 20 | Proof of Elapsed Time (PoET) [79] | Permissioned/Permissionless | Hyperledger sawtooth | Python, Javascript, Go, C++, Java and Rust | Cheap participation | Special hardware, Not suitable for public blockchain |
| 21 | Proof of Capacity (PoC) [21] | Permissionless | Burstcoin, Chia and spacemint | Java | Efficient, Distributed, Cheap, Utilizes free dik space as a resource | Decentralization issue |
| 22 | Proof of Existence (PoE) [80] | Permissionless | Poex.io, Hero Node, Dragon Chain | Not known | Document time stamping, Document integrity | Not known |
| 23 | Proof of Authority [81] (PoAuthority) | Permissioned | PoA.Network, Ethereum, Kovan testnet, vechain | Solidity, Java, Python | Reduced maintenance costs | Centralization |
| 24 | Ethash [82,83] | Permissionless | Ethereum | Python, Go, Java, Javascript, Ruby, C++ | Avoids 51% attack | Memory intensive, Needs computers with powerful GPUs |
| 25 | Proof of Stake Velocity (PoSV) [84] | Permissionless | Redcoin | Not known | Reduces the time wastage of mining, Removes mining arms race | Not known |
| 26 | Proof of Space Time (PoST) [84] | Not Known | Filecoin | Go, Javascript | Cheap computationaly | Needs more interaction |
| 27 | Federated Byzantine Agreement (FBA) [85] | Permissioned/Permissionless | Steller and Ripple | C/C++, Javascript, Go, Java, Node.js | Less participants to achieve consensus' Robust | The parties must accept the exact number of candidates |

#### 5.1.1. Proof of Work (PoW)

Proof of Work [67] is the first consensus protocol used by a public blockchain. All the nodes need to solve a cryptographic puzzle by brute force. The node which wins the puzzle is rewarded and all the other nodes computations are wasted. The consensus is achieved as 51% of power.

#### 5.1.2. Delayed Proof of Work

This protocol is designed as a hybrid consensus in which one blockchain takes security from another blockchain through hashing power [68]. A group of nodes are responsible for adding data from the first blockchain onto the second. Both blockchains would then compromise to undermine the security of the first blockchain. Komodo which is attached to the bitcoin blockchain was the first to make use of this protocol.

#### 5.1.3. Proof of Stake (PoS)

- Original PoS: Proof of stake uses the wealth of miners to win a ticket rather than computational power. PoS was first implemented in 2012 as cryptocurrency PeerCoin. PoS is kind of a hybrid design where PoW is used in the beginning for coin minting and later PoS is used for the security of the whole network. PoS works with the concept of a coin's age which is explained by example. If there are 10 coins which are held for 10 days its age is 100 days. If these coins are spent, their age is consumed. In PoW the main chain with most work is followed, and in PoS a chain with most coin age is followed.
- Cardano's Ouroboros: This protocol adds security measures to ensure persistence and liveness within the system. This implementation elects the stakeholders through a delegation process and takes the snapshots of current stakeholders labelled as an 'epoch'. The subset of current stakeholders randomly decide who will be the next epoch stakeholder.

#### 5.1.4. Stellar Consensus Protocol (SCP)

This is a decentralized consensus protocol in which nodes have the ability to choose which nodes to trust. This group of trusted nodes is known as "quorum slice". An agreement is reached by a set of nodes called quorum whereas quorum slice is a subset of a quorum which selects one particular node for an agreement. SCP proposes new candidate values for agreement via a "nomination protocol". Each node will then vote for a single value among these. After this a "ballot protocol" is implemented. In this phase the nodes vote for the previous values to keep or abort them. In case the quorum slice does not reach consensus the value is shifted to a higher valued ballot so that it can be voted on again.

#### 5.1.5. Delegated Proof of Stake (DPOS)

Another form of PoS is delegated proof of stake (DPOS). It is the same as POS except the stakeholders elect their delegates to generate and validate the blocks. As there are fewer nodes to validate, blocks can be validated quickly and the transactions can be confirmed quickly. Delegates can tune the block size and intervals in the meantime [69].

#### 5.1.6. Leased Proof of Stake (LPoS)

Leased Proof of Stake (LPoS) allows the nodes with low balance to participate in solving the blocks [70]. The nodes with low balance takes some amount on lease from the nodes with high balance. The amount is in the control of the wealthy owner. When a block is solved by these nodes the reward is shared with the wealth holders. This approach is more decentralized hence making the blockchain more secure.

### 5.1.7. Byzantine Fault Tolerance (BFT)

When nodes can generate arbitrary data, byzantine fault tolerance (BFT) is a replication algorithm that can solve the issue of reaching consensus [71]. BFT can guarantee the liveness and safety of a system. It can tolerate up to 33% of faulty nodes [72].

### 5.1.8. Directed Acyclic Graph (DAG)

In directed acyclic graph (DAG) the data is stored topologically in graph manner. DAG can overcome the problems of data processing, compression and routing. One of the disadvantages of PoW is the creation time of the block which is 10 min. DAG instead of implementing a single chain, works on "side chains" [73]. Therefore, to reduce the time of block creation and validation different transactions are performed on multiple chains. Mining also is a waste of time and energy so in DAG all the transactions are maintained and directed in a certain sequence. DAG is acyclic so there is no chance of finding the parent node as it's a tree of nodes and not the loop of nodes. Some of the basic concepts of DAG are:

- No More Double Spending: In traditional blockchain, a scenario of more than one miner tries to validate the same blockchain leads to double spending. This also leads to hard or soft forks. The DAG is safer and robust as it validates a particular transaction based on the previous number of transactions.
- Less Width: The transaction in another consensus algorithm gets added to the whole network but in DAG the transaction is added to the transaction graph. This makes the whole network less bulky and easy to validate a particular transaction.
- Smarter and Faster: As the blockless nature of DAG, it is much faster than PoW and PoS.
- Favorable to the Smaller Transactions: Bitcoin and Ethereum are not much friendly for the smaller amounts rather DAG seems perfect as transaction fee is neglected.

### 5.1.9. Proof of Weight (PoWeight)

This is a very good alternative to PoS. In PoS if the participant has more tokens, he is the winner of the block but this idea makes it a bit biased [74]. So to solve this problem of biasedness PoWeight was introduced. It works on other factors than on tokens. Cryptocurrencies like Filecoin, Algorand and chia implement this algorithm. The factors are known as "Weighted Factors". In Filecoin the Interplanetary File System (IPFS) data that a system has is the weighted factor. There are also some other factors like Proof of Reputation and Proof of Spacetime. The proof of weight system provides scalability and customization, however incentivizing it can be a big challenge for this algorithm.

### 5.1.10. Delegated Byzantine Fault Tolerance (DBFT)

Delegated byzantine fault tolerance (DBFT) is a different version of BFT. This fault tolerance algorithm divides P2P into two types' ordinary nodes and bookkeepers. Bookkeepers are elected by ordinary nodes who vote for the book keepers to take part in the consensus process. A random book keeper broadcasts its transaction to the network and other 66% bookkeepers should agree on the validation of transaction data. Upon validation the transaction is appended to the blockchain. For another consensus process another book keeper is selected via the same process [75].

### 5.1.11. Ripple Protocol Consensus Algorithm (RPCA)

Ripple cryptocurrency uses this algorithm and it was designed to address other algorithm latency issues. RPCA works as follows:

- Each server puts all the valid transactions in the "candidate set" which is the public list.
- Each server gathers all candidate sets, from other Ripple servers which is found in its unique node list.
- Each server votes for the validity of transactions. This voting can be done in one or multiple rounds.

- A minimum of 80% yes is required for all the transactions in the final round to be written into the public ledger and then the ledger is closed [76].

#### 5.1.12. Proof of Importance

Proof of Importance (PoI) is used by the cryptocurrency New Economic Movement (NEM) [75]. NEM is a blockchain project which has created decentralized digital platform used by decentralized applications, and a digital asset having the same name. It was evolved in March 2015 by Singapore-based non-profit organization by the name of NEM.io Foundation. Every account has a vested and unvested XEM balance. Unvested balance is the amount received.

NEM is a blockchain project which has created decentralized digital platform used by decentralized applications, and a digital asset having the same name. Every account has a vested and unvested XEM balance. Unvested balance is the amount received. After every 1440 blocks one tenth of the unvested balance goes into a vested account. XEM is spent from both vested and unvested accounts when a XEM needs to be sent. This is so because both accounts need to retain the same ratio; 10,000 XEM is the minimum amount an account should hold in its vested part in order to be eligible for "Importance Calculation". Importance is calculated on a weighting factor i.e., to check if an account is a part of cluster nodes or an outlier, on amount of vested XEM, the rank of the account within the network. Ranking is held via the NCDawareRank algorithm and NEM network determined two suitable constants.

#### 5.1.13. Proof of Exercise (PoX)

This algorithm is also used for cryptocurrencies. As in proof of luck the computational power is reduced. Proof of exercise uses the computational power for scientific problems. In proof of exercise the employers give the matrix based problems to miners. There are two reasons for using matrices: tuning of the network difficulty becomes easy and they are a principal abstraction for many scientific problems. A "hostage credit" system is placed in the system so that the data for matrices required are readily available. Miners need to bid for a problem to solve and deposit which will be refunded after successful completion of the problem. A sum should be deposited by an employer which should have a greater total cost than the cost of storing the matrix data. The miners send the solution of the problem to the verifiers. Verifiers use a probabilistic verification scheme to verify the data before it is committed to the blockchain. To avoid complicity among miners, verifiers and employers the matrix problem is sent via a shuffling service. This is done either directly after the miner sends the data for verification or directly after the matrix data is being published by an employer. In addition if the bid is won by multiple miners at the same time the coin reward is shared.

#### 5.1.14. Proof of Ownership

Proof of work is prone to Sybil attack where an attacker can do the amount of work multiple times as he acts as multiple participants [75]. Using a Trusted Execution Environment (TEE) a participant needs to own a unique Central Processing Unit (CPU) instead of virtually maintaining participants. An Enhanced Privacy Identity (EPID) signature is used in this protocol which produces pseudonyms which show if the multiple proofs are coming from the same CPU. The algorithm generates unique pseudonyms so that if a malicious user resets the owner epoch register for using it multiple times, the attacker may not be able do that. Therefore, a consensus in blockchain is reached by following a block having most proofs with unique pseudonyms.

#### 5.1.15. Proof of Luck (PoL)

Proof of luck aims to increase transaction throughput and reduce the computational power used by PoW. Each block when mined is given a random number between 0 and 1 which is called a "luck value". Higher numbers are considered as luckier and less unlucky.

The highest luck value is calculated by adding all the values of each block starting from genesis block till the last block. The miners prefer to append their block to the blockchain having the highest luck value. A higher luck value produces less delay and optimizes communication within the system. The original miner will not need to broadcast its block to the network as another miner tries to solve the proof on the first block having higher luck value [77].

#### 5.1.16. Proof of Activity (PoA)

There are many disadvantages of proof of stake which includes keeping coins for long with oneself [75]. Coins are also sent to the transactions which further assigns coins to the rest destroying the coinage but they are not included in PoS. When the node is offline, coins are still collected and this is the main weakness of PoS. When the node is occasionally online, there is a delay in receiving their incentive which results in incentive distributions bursts. If the amount of online nodes are insufficient it may result in attacks.

#### 5.1.17. Proof of Publication (PoP)

Blockchain provides hashes which are linked together; however, the servers may backdate the records by hashing and signing the past timestamps. To handle this issue the timestamps are lined together. This technique takes the timestamp of the digital record's creation and modification, takes a hash out of record and timestamps and links them together. So even if the clocks are incorrect, this technique can give certainty to the complete order of records.

#### 5.1.18. Proof of Burn (PoB)

Proof of burn (PoB) is also known as PoW without energy waste. The miners instead of using heavy power utilizes virtual token coins to burn and destroy in order to get a right to write into the blockchain. The miners buy mining rigs which gives them power to mine blocks. Miners can send and get transactions by burning their own and others coins respectively. More coins burnt results in more virtual mining rigs.

#### 5.1.19. Proof of Retrievability (PoR)

PoR provides mining resources with the additional ability of distributed storage of archival data. It is similar to PoB but it does not just involve computational power but also storage. This consensus is more suitable for cloud computing where a file system (Prover) can give surety to a client (verifier) that the file is intact. PoR is well known for permacoin and koppercoin [78].

#### 5.1.20. Proof of Elapsed Time (PoET)

In proof of elapsed time (PoET) each node is given a randomized timer object from a trusted code. The node having the shortest timer is when expired the node wakes up, propagates a signed certificate to show this node is the block leader. The timer is given randomly so that the malicious user does not try to continuously get a shortest timer [79].

#### 5.1.21. Proof of Capacity (PoC)

Also known as proof of space. Instead of using miner's computational power, mining devices storage capacity is used to store the possible solutions for mining cryptocoins. The more storage space results in higher chances of winning the mining reward. The list of solutions is stored on the device hard drive before the mining process begins.

#### 5.1.22. Proof of Existence

Traditional models of validating the documents are based on central authorities which can lead to security breaches [80]. Through blockchain the document can be stored with a signature and timestamp associated with a legal document. The user can validate the document anytime. This is also advantageous as the blockchain is not centralized so the user can get the privacy and security by having the proof of the document as decentralized where it cannot be modified by a third party.

#### 5.1.23. Proof of Authority

Proof of authority was proposed for private networks as part of the Ethereum ecosystem. In PoA, authority is given to N nodes. Each node is given a unique id. These authorities are responsible for running the consensus and ordering the client's issued transactions. PoA runs on a mining rotation schema in which the responsibility of block creation is distributed fairly among the authorities [81].

#### 5.1.24. Ethash

Ethash is a memory-intensive proof of work algorithm which is used by Ethereum [82]. In bitcoin, a block is created after every 15 s approximately as the difficulty level is adjusted automatically. However Ethereum depends on mining of a 1 GB data set and these data sets are produced out of the headers of previous blocks after every epoch. i.e., after about every 5.2 days or 30,000 blocks. The clients of Ethereum store and generate the future data set in advance because the data set can take a long time to generate. This can prevent delay in mining at the beginning of every epoch. Using block's header mining is one on the nonce and subset from the data set. The SHA3-256 hash of this subset is compared to some threshold, if the hash is less than the threshold, its nonce is valid and the block is appended to the blockchain. Ethereum designed Ethash with an aim of being an "Application Specific Integrated Circuits (ASIC)-resistant" mechanism of which reduced the advantage of joining mining pools. Since blockchain mining centralization can introduce a risk of 51% attack. So Ethereum relies on memory instead of computational power. This also makes ASICs less attractive, as graphic cards of top range are capable of mining Ether [83]. Currently, Ethereum is moving from PoW to proof of stake due to the difficulty in entering the miner system. So the the protection against attacks is more than the PoW.

#### 5.1.25. Proof of Stake Velocity (PoSV)

This is used in red coin cryptocurrency. It is a bit alternate to proof of work (PoW) and PoS. The ownership is referred to as stake and activity is referred as velocity. It is based on the frequency at which a currency unit is used in the economy in a given time period. The higher velocity is a sign of a better economy. Here is the formula to achieve proof of stake stake velocity: Vt = nT/M Here 'Vt' is the currency unit's velocity, 'nT' is the aggregate for transactions while 'M' is the amount of money in circulation [84].

#### 5.1.26. Proof of SpaceTime (PoST)

In proof of spacetime (PoST) a prover has to convince a verifier that data and space has been stored by him/her over a period of time. This data and space storing over a period of time is known as "spacetime" resource. PoST uses less energy as compared to proof of work as it requires that the difficulty level be increased by prolonging the time period in which the data is stored rather than increasing computation costs [85].

#### 5.1.27. A Federated Byzantine Agreement (FBA)

A federated byzantine agreement (FBA) is well known for its low transaction costs, scalability and high throughput. Steller and Ripple cryptocurrencies use this consensus where Steller was the first one to use FBA. It works like a byzantine fault tolerance where a blockchain is a responsibility of each byzantine general which belongs to the same blockchain. Nodes need to be known and verified in advance before the user requests any enactment from the FBA [86]. The notary node selects those nodes who they trust, making quorums of nodes and hence forming the FBA network.

### *5.2. Healthcare Based Consensus*

Blockchain is helpful in healthcare as it provides security to the medical records and other security breaches which healthcare faces on a daily basis. Figure 6 shows the patient profile over the blockchain which can be used for information by the concerned doctor, hospital, insurance company or it can be used in the supply chain management.

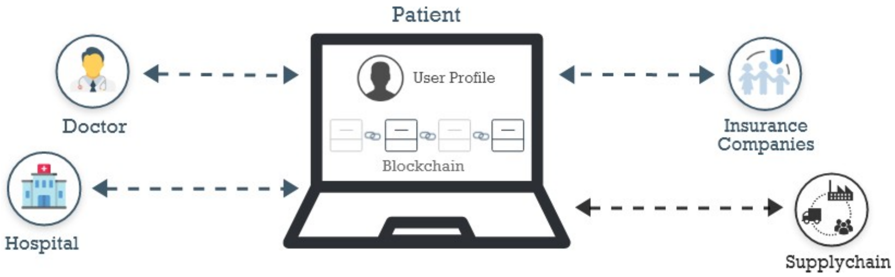

**Figure 6.** Blockchain in healthcare.

The consensus algorithms used in healthcare are discussed below.

#### 5.2.1. Proof of Interoperability

Proof of interoperability removes some of the disadvantages of proof of work. This is designed to achieve something fundamentally valuable. This protocol verifies that the incoming messages are interoperable with the known set of semantic and structural constraints. For the use case discussed by Kevin Peterson and Rammohan Deeduvanu in their research work is the FHIR profile (Fast Healthcare Interoperability Resources). This is an evolving standard that shows elements and data formats, along with providing publicly accessible application programming interfaces (APIs) for the reason of exchanging Electronic Health Records. Proof of Interoperability requires a network to reach consensus on the set of allowed FHIR profiles which includes the value sets of the attendant as well. This type of consensus requires a human-based process to reach. Participants negotiate with the help of clinicians and terminology specialists. This consensus cannot, however, be reached programmatically. Network agreement is most likely a human-based process, where network participants negotiate and collaborate with the help of both terminology specialists and clinicians. This collaboration demands a centralized repository. The value set repository proposed in this paper is the value set authority center (VSAC) [87]. A privacy-preserving medical system for data sharing based on Hyperledger Fabric (MedHypChain) proposed by [88]. The authors show that MedHypChain achieves anonymity, confidentiality, unforgeability and traceability. They also facilitates the patient to manage its information regarding health in the blockchain whereas it can be accessed by an authorized entity.

#### 5.2.2. Proof of Disease

There are several steps in PoD which are as follows:

1. Mobile devices and desktops are used as user devices and the server is cloud based application. Server and client communication is done via Java Script Object Notation (JSON) objects.
2. The patients enter their details of disease in simple English and the server runs hunspell using corpus (customized medical dictionary) over the user text.
3. The user text is parsed using metathesaurus and UMLS and then the text is converted into multiple UMLS (Unified Medical Language System) CUI (Concept Unique Identifier).
4. UMLS CUI is converted into ICD10 and SNOMED CT (Systemized Nomenclature of Medicine—Clinical Terms) Codes.
5. The important information is either taken from the user online if the information is not available in EMR/HER (Electronic Medical Record/Health Electronic Record).

6. Using graph analysis merge SNOMED CD with phonemics databases to determine the fundamental disease concepts in machine understandable ontologies.
7. The medical specialists called Medical Miner (MM), validates and confirms all the results from the above steps and commits into the blockchain.
8. Additional biological databases are added and repeated over in cases, when the proof of disease cannot be determined. These are big-data databases Gene Ontology, Human Phenotype Ontology (HPO), Virtual Metabolic Human etc. [89].

#### 5.2.3. Medical Information Sharing Using PBFT (Practical Byzantine Fault Tolerance)

As discussed by Jieying Chen [90] PoW utilizes much energy and resources so instead of PoW they used PBFT in their application of blockchain for medical information sharing. PBFT can tolerate one third of nodes to be malicious hence it is much more efficient in reaching consensus than PoW.

### *5.3. Intelligent Transportation System (ITS) and Vehicular Ad Hoc Networks (VANETS) Consensus Algorithms*

Recently smart vehicles have gained much attention in the area of research. A vehicular network is composed of various sensors, on board units (OBU) and road side units (RSU) etc. where communication is exchanged among the nodes. Security issues may arise when an adversary tries to forge the message or tries to divert the traffic in case of platoon. Blockchain helps in securing the communication as all the communication is being done via transactions where they are recorded in a distributed ledger. There are consensus algorithms discussed in different scenarios of vehicular ad hoc networks (VANETS) and intelligent transportation systems (ITS). Figure 7 shows the general concept of blockchain in VANETS.

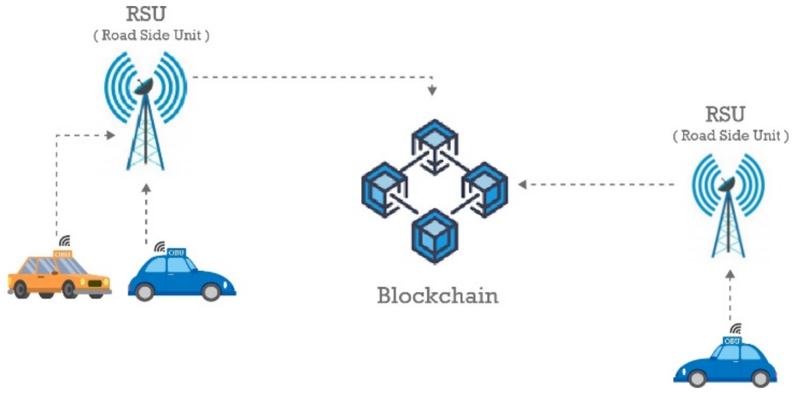

**Figure 7.** Blockchain in vehicular ad hoc networks (VANETs) [91].

#### 5.3.1. Proof of Movement

Road miners (smart phones or computers etc.) share their transportation data with the community and get automatic reward (Tokens) called zooz. These tokens can be used to pay for ride sharing and other services. Road miners get more rewards if they drive for long (Incentive layer) [92].

#### 5.3.2. Proof of Driving

Proof of driving (PoD) validates and verifies the vehicles in communication. IV-TP (intelligent vehicle trusted point) is the crypto data which is assigned to each vehicle and if a vehicle wins the consensus competition, it gets more IV-TP from the benefiter IV. The vehicle having more IV-TP is leading the vehicle's communication network. This way it creates a trusted environment between vehicles communication [93].

### 5.3.3. Proof of Reputation

The paper discusses in this section a decentralized reputation-based blockchain in vehicular networks. The received messages are rated by the elected vehicle from the crowd and then broadcasts its ratings which are in the form of block. Using a vehicle's local knowledge they validate the block and decide to add the block to the blockchain or not. Thus the rating which are stored on the blockchain are said to be reliable enough as these are validated by most of the vehicles in the network [94]. Proof of reputation can also be used generally for almost any business network. Gochain uses proof of reputation for Dapps (Decentralized Applications) and smart contracts that aims to decrease energy consumption, increase performance, provide network security and decentralization.

## 5.4. Consensus in Supply Chain

Supply chain is the service of producing goods and products and delivering to the ultimate customer. It deals with the manufacturers, suppliers, warehouses, organizations, retailers and distribution centers where raw material is changed into fine deliverables. Blockchain has revolutionized the supply chain process drastically by reducing delays, costs and human errors. All the changes made during the process of a supply chain are recorded in the transactions ledger keeping it secure and unchangeable. In Figure 8 the supply chain process is described where raw material is packed with a RFID (Radio Frequency Identification) tag and barcode is used to finish the goods.

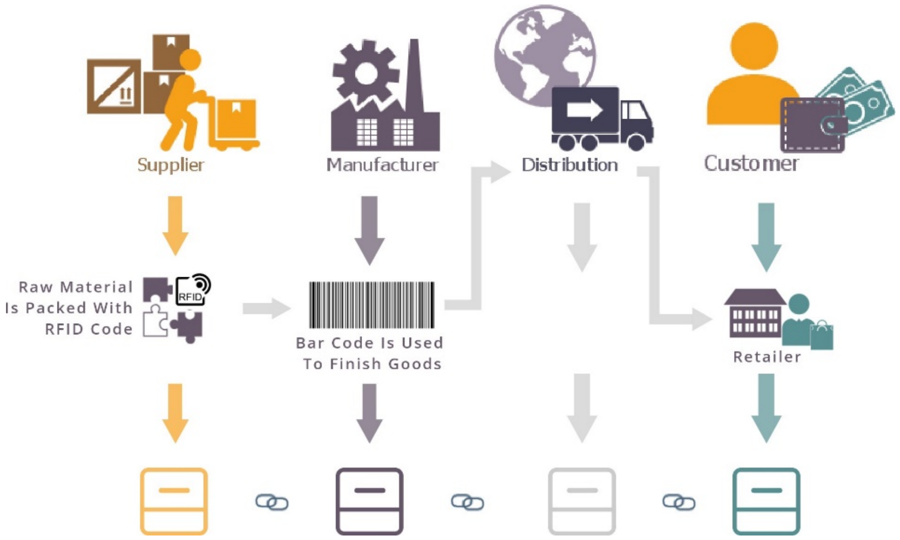
Supplier
Manufacturer
Distribution
Customer
Raw Material Is Packed With RFID Code
RFID
Bar Code Is Used To Finish Goods
Retailer

**Figure 8.** Blockchain in a supply chain [95].

### 5.4.1. Soft Consensus-Based Group Decision Making

Acting in an isolation for the decision in supply chain cannot be that helpful than making joint decisions of planning and execution using supply chain coordination (SCC). A methodology named a fuzzy TOPSIS (Technique for Order Preference by Similarity to Ideal Solution)-based MCDM (Multi Criteria Decision Making) for selection problems of SCC is proposed in this paper. As the decision makers are separated geographically, they give their preferences via the internet. A consensus should be reached for the preferences among the decision makers and in this regard this paper presents a soft consensus-based GDM (Group Decision Making) methodology. All the supply chain partners reach a consensus by forming a decision matrix. This is an objective weight determination methodology which is used for assessment of the weights of the criteria without mediation of the decision makers. This methodology is used as the meeting is internet based [96].

#### 5.4.2. Weight-Based PoS

As discussed by Leng Kaijun [97], a public blockchain consensus has slow speed. The selective incentive weight should be used in common for the agricultural business resources so that these resources reach the underdeveloped and remote areas. Therefore this paper presents a consensus algorithm for the blockchain of agriculture business resources. The algorithm considers weight based on PoS.

### *5.5. Consensus in Internet of Things (IoT)*

IoT relies on a centralized system where many devices are attached to each other via the cloud or any other central system [98]. The data are sent back from the cloud to the device. This makes the scalability issue as sending and receiving of data from many devices can slow up the central system and security issues may arise. Blockchain has made the IoT more reliable, secure and efficient. IoT produces a massive transaction so a decentralized solution would provide a cost effective solution and a peer to peer communication can provide a standardized management for the massive transactions. Although a peer-to-peer communication model suffers a security challenge but the blockchain technology achieves transparent interactions among different parties. The use of a Proof of work consensus algorithm makes the blockchain distributed ledger more trusted and secure [99].

Figure 9 shows the scenario of blockchain retrieving data from various IoT devices. In different scenarios of IoT and blockchain different or already discussed consensus of the blockchain are discussed below.

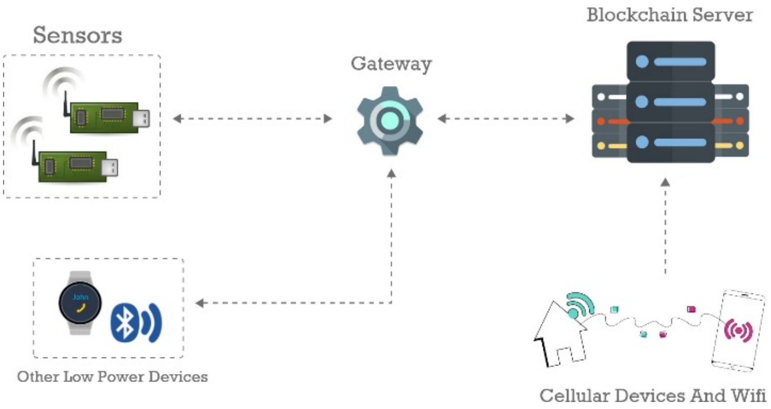

**Figure 9.** Blockchain in Internet of Things (IoT).

#### 5.5.1. A Distributed Consensus Algorithm

Global consensus might be the need to facilitate service integration and knowledge sharing. In this paper an idea of local consensus is developed and this is developed by each of IoT edge nodes when needed. Clusters are formed out of network nodes and each cluster reaches a local consensus. This local consensus can be used to make consensus decisions in integration of functional capabilities and knowledge sharing. Any service can become part of the service pool where a local consensus is achieved for all the edge nodes involved in IoT. The proposed matching value-based methods helps in finding the possibility that the existing services can lead to the composition of new services by the existing IoT services. Therefore, the matching values form the nodes are gathered and synthesized to reach a decision which would be acceptable to all. This is helpful in not only to achieve better solutions but also to create trust among nodes and clusters of the network [100].

#### 5.5.2. Consensus Protocol of Diversified Services of Complex Internet of Things Applications

The consensus protocol discussed is the merger of proof of stake and proof of work. Ethereum Casper FFG (Friendly Finality Gadget) [100] uses the same protocol. The implementation of the protocol begins with the genesis block. An appointing committee should be organized which will pay the deposit prior. However the amount to be deposited depends on the actual situation. Instead of each common block this paper focuses on the checkpoint blocks. Members vote for the final winner of the fork. The period in which voting takes place is called an epoch. The appointing committee members can also issue transactions just like other nodes of the network. Additionally they have the charge of voting at justified checkpoints. Ballots are used by the members in voting where they decide which checkpoint block should be included in the main graph. Then the result of the vote is broadcast to the whole network. If Block checkpoint 1 (BCP1) gets more than 2/3 ballots, the block is acknowledged and prepared and the epoch ends. The transactions that are in leaf blocks and those incompatible transactions are sent to the pool for further processing. In the next cycle BCP1 is committed and finally confirmed once BCP2 is voted and said to be prepared.

### *5.6. Consensus in Big Data*

Bitcoin is the most known application of blockchain and yearly its size has increased by 15 GB. Since blockchain is a transaction database distributed among multiple nodes which sort of push it to the big data territory. Figure 10 shows a general picture of big data in blockchain. Blockchain itself has been used in big data architecture using its own consensus protocols.

**Figure 10.** Blockchain in big data.

#### 5.6.1. Paxos Algorithm for Consensus

Paxos is a decentralized consensus algorithm which lets nodes communicate through an asynchronous network. This algorithm is designed in a way that any value accepted by majority will not be changed so that all the nodes have the same copy of the value [101].

#### 5.6.2. Proof of Collaboration

The proof of collaboration is used in "Making Big Data Open in Edges: A Resource-Efficient Blockchain-Based Approach" here if an edge device (node) intends to generate new block it will have to show the collaboration from other edges rather than solving puzzles. This requires less computation power than puzzle solving.

### *5.7. Consensus in Cellular Networks*

Blockchain offers great opportunities for different platforms and applications. Mobile networks can also use blockchain as a part of the infrastructure which will provide verifiable and secure digital transactions and can also improve privacy.

### *5.8. Proof-of-Location (PoL)*

In cellular network blockchain mobile phones are considered as nodes. The geographical location of a node at certain time is attested by a digital certificate, which is known as proof of location. The proof of location consensus is required to achieve the proof of location certificate. In proof of location consensus there is a "Prover" node and a "Witness" node. The prover node collect proof of location from its close neighbor devices through short range communication technologies. The witnesses are those nodes which provide a proof of location to the prover [102]. Figure 11 describes the scenario.

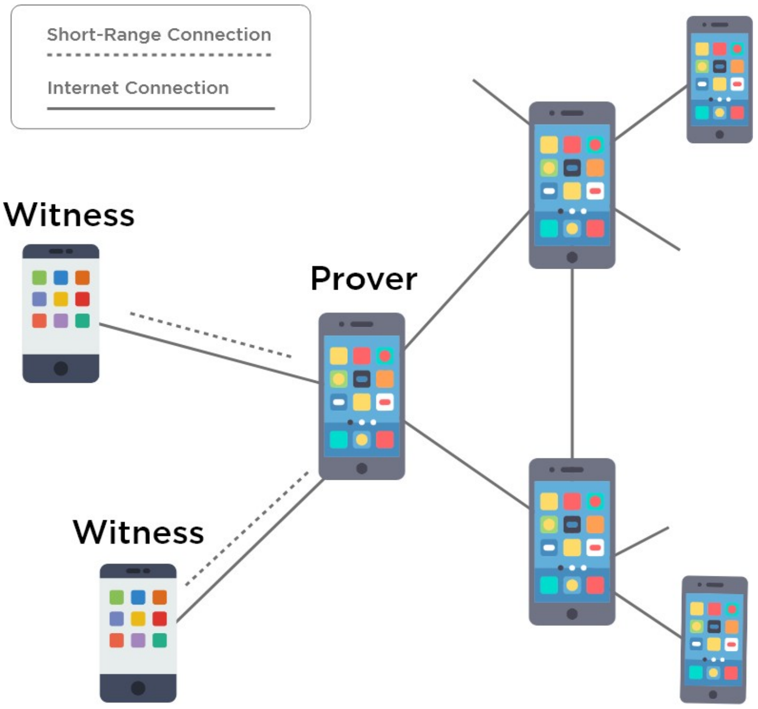

**Figure 11.** Proof of location.

### 5.9. Consensus in Social Networks

Social networks are rapidly producing personal data. According to a recent report Facebook which is the largest social network has collected personal data of 300 petabytes since its foundation. Blockchain is a viable solution to protect data by providing decentralized privacy.

#### Proof of Credibility

The contractor signs contracts with different parties and the number of these parties is known as measuring credibility score. A miner in this consensus of blockchain provides proof that he has a high credibility score. This proof is actually an improvement of the previous work of researchers, in which the trust score was on how many good actions a node has made. The improvement calculates the connection between nodes by credibility score. Instead of using a proof of stake the credibility score gives a problem that even if a contract is true or fake the credibility score is added. An attacker can succeed in a 51% attack if he makes fake contracts with false parties in order to increase his credibility score. Later this attacker can join the true parties who will renew the contracts illegally. To settle this issue, a hybrid of proof of credibility and proof of stake is used in this proposed methodology where these proofs are executed alternately. If a miner generates a block using proof of credibility, the next miner will generate a block using proof of stake [103].

### 5.10. Consensus in Distributed Web Services and Storage

When cloud storage and web services are made permissionless, decentralized and secured, it can bring a positive change in standards of unit economics of decentralized storage. Human capital costs as well as high mark-ups will be eliminated. Solana aims to bring this trend to the future of blockchain by introducing a scalable consensus called proof of history (Available: https://iconetwork.io/tag/proof-of-history/, accessed on 14 March 2020).

#### Proof of History

Each transaction in a network is time stamped. This protocol verifies the order and duration of time between events. Leaders are designated by the system that can organize and send the user messages to other nodes for further processing. Verifiers execute the transactions and publish the confirmed transactions using computed signatures. These confirmed transactions are actually votes for the consensus algorithm.

Proof of History (PoH) works in collaboration with Proof of Stake. Leader produced current sequence is confirmed using PoS. Next leader selection via voting is also done using PoS. It can also be used to punish any verifier that acts against the agenda of the network. There is an additional layer of security in this network that generates an invalid hash at random intervals and those verifiers who validate it are penalized.

### 5.11. Consensus in Governance

Blockchain can be used in governance though it cannot take full control from the central body but it can be part of it. Being the part of governance blockchain can be used in areas such as voting, transparent budgeting, replacing paper-based systems, secure data entry shown in Figure 12. There are other areas where blockchain can be used, such as digitizing the currency by using cryptocurrency instead which might never be accepted and implemented. There are a lot of consensus protocols such as proof of work and proof of stake stack that can be used in blockchain in governance.

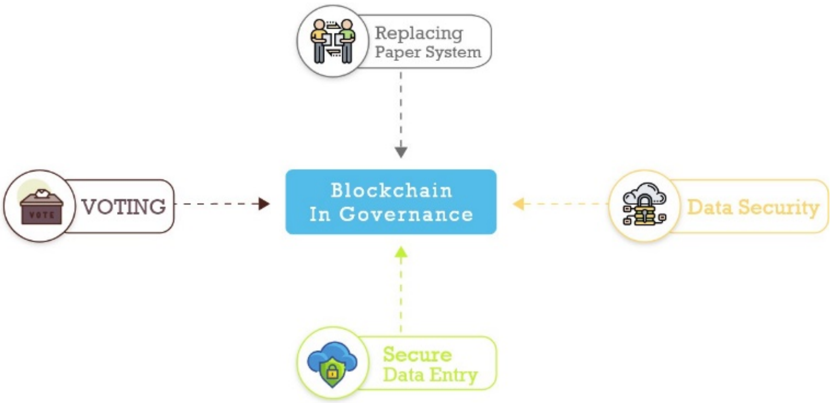

**Figure 12.** Blockchain in governance.

### 5.12. Consensus in Entertainment

Blockchain is also very useful in entertainment business such as “Music on the Blockchain” [104] which protects the copyright information of music by storing it on blockchain. The proof of work and proof of stake stack consensus algorithms are discussed for the implementation of music on the blockchain. More applications of blockchain in entertainment are shown in Figure 13.

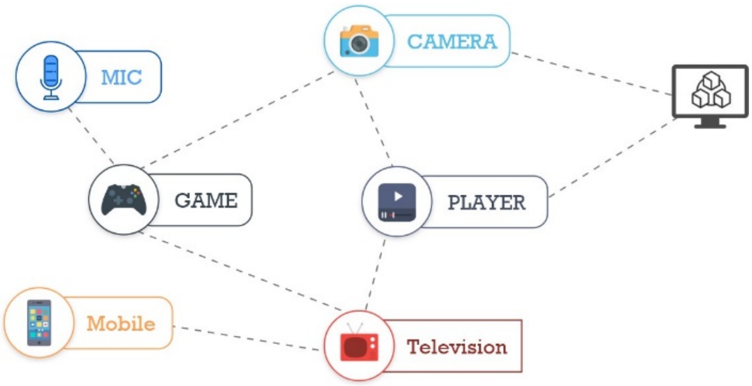

**Figure 13.** Blockchain in entertainment.

### 5.13. Consensus in Real Estate

Blockchain can be implemented in real estate such as recording of properties titles and deeds [105]. To ensure the safety of the data it is designed to be stored in blockchain and to ensure safe transactions on that blockchain proof of work consensus has been favored. Also for digitizing the land record system by blockchain [106] would make it secure from corruption. The proof of existence is advised to be used for the intellectual properties. Other than that proof of concept is also used in blockchain for real estate [107]. The general image for real estate over the blockchain is shown in Figure 14.

**Figure 14.** Blockchain in real estate.

### 5.14. Consensus in Power

Blockchain is going to change the legacy systems of centralized nature by hybrid distributed systems which are made up of solar power micro grids and large power plants. This kind of distributed energy system will be a reliable, efficient and renewable energy delivering system. There is also a possibility that blockchain may change the trading system and businesses would trade off using electricity for example if a factory needs additional power, it can buy unused electricity which another factory is selling for five minutes. These five minutes are actually the unused downtime minutes of a factory. This kind of trade can give efficiency benefits to grid operators.

Each home is installed with a smart meter (SM) in order to achieve better scheduling in the smart grid. These SMs collect real-time data of electricity consumption and utilities use this data to provide smart home services in a better way. The real time data can disclose private data of the user and an adversary can take advantage of this data by reading the usage patterns of the electricity consumption profile of the user. In [108], a privacy-preserving and data efficiency aggregation scheme is proposed via blockchain. Users are divided into groups and a private blockchain is managed by each group for its members. For privacy preservation inside a group each user uses pseudonyms to hide their identity. In addition, proof of work is used to achieve block verification. The said scheme achieves security requirements and better performance than other methods.

### 5.15. General Consensus Algorithms

The algorithms discussed in this section are general purpose which can be used for any type of asset. Table 4 has some of the important features of the general consensus algorithms.

**Table 4.** Features of general consensus algorithms.

| S.No | Consensus Algorithms | Permissioned/Permissionless | Platform | Applications | Programming Language | Advantages | Disadvantages |
|---|---|---|---|---|---|---|---|
| 1 | Proof of Vote [109] | Permissioned | Not Known | Consortium Blockchains | Any programming language can be used | Consistency, Availability, Partition tolerance | Problem in modular design and parallel processing |
| 2 | Tendermint [110] | Permissioned | Cosmos, Ethereum | ABCI (Application Blockchain Interface) | Rust, Go, Haskell, C/C++, Java etc | Does not require mining | Unfair |
| 3 | Proof of Human Work [111] | Not known | Humancoin | Cryptocurrency, password protection, Bot detection) | Not known | Fair | Requires an initial trusted setup, Prone to malicious attack |
| 4 | Simplified Byzantine Fault Tolerance [112] | Permissioned | Chain | Financial Applications | Java, Node, Ruby | Good security, Signature validation | Not for public blockchain |
| 5 | Practical Byzantine Fault Tolerance [112,113] | Permissioned | Hyperledger, Zilliqa | Cryptocurrency and other asynchronous systems | Golang, Java | High transaction throughput | Centralized |
| 6 | Raft [114,115] | More suitable for Private/Permissioned Blockchains [62] | Kaleido, IPFS Private Cluster, Quorum | CockroachDB | Go, C++, Java, Scala and Rust | Supports configuration changes, Simple and easy as compared to Paxos | Centralized |
| 7 | Proof of Proof | Not known | Veriblock | Not known | Not known | Security inheriting | Provides potential attack vectors |
| 8 | Proof of Believability | Not known | IOST | Not known | Not known | Fast finality and more decentralized than PoS, Scalability | Not known yet |
| 9 | Proof of Property [116] | Not known | Ethereum | Not known | Not known | Scalable, Save a lot of local space | Forking may create issues |

### 5.15.1. Proof of Vote

A proof of vote is built for consortium blockchain where companies develop a partnership and each company represents an officer [109]. These companies share their business-related data via coalition committee. Business transactions and operations are recorded on blockchain. The companies do not agree on giving right to any of the companies to produce a block so they decided to hire a butler team. The team is hired from all over the world and the election is held among them on a regular basis. The blocks are produced by the team and are sent to the companies for verification and voting which makes the power decentralized among the team responsible for producing blocks and each block will be submitted to each company for verification and voting, making the power decentralized within the partnership committee. In order to maintain reliability, safety and efficiency the butlers are paid high salaries by the companies. Anyone can join the butler team but the team member is recommended by the coalition and they have to submit a deposit. The members of the coalition supervise the work of a butler and they are graded accordingly so that only the honest ones can survive. Therefore, PoV is a consensus method proposed for consortium blockchain which is maintained by organizations and enterprises in different areas of the world.

### 5.15.2. Tendermint

Tendermint is a permissioned consensus algorithm. It is the same as PBFT as it can tolerate one-third malicious nodes [110]. In the tendermint protocol the participants are known as validators which vote on their proposed blocks. There are two steps of voting: pre-vote and pre-commit. When more than two third of validators pre-commit in a same round for the same block, it is then added to the blockchain.

### 5.15.3. Proof of Human Work

Puzzles related to human work are very much similar to PoW except that a human is involved in finding a solution [111]. The problem solver should not be a machine only and this is the main difference between PoW and PoH. A puzzle should be made hard to solve for humans and uneasy to solve for machines. Although we expect the verification to be easy for machines as in PoW.

### 5.15.4. Simplified Byzantine Fault Tolerance (SBFT)

In simplified byzantine fault tolerance (SBFT), a block gathers all the transactions, batch them and validate them in a new block [112]. All the nodes follow the rules of a block generator to validate all the transactions. A block signer validates these transactions and adds its own signature. So if any of the blocks miss one of the keys, it is rejected. This algorithm uses an adopted version of a Practical PBFT consensus algorithm. This protocol is also aimed to provide improvements over PoW. There is a single validator who is a known party and the nature of the ledger is permissioned. The validator forms a new block with a bundle of proposed transactions. Consensus is achieved when a minimum number of nodes approve a block. The number of nodes to reach consensus is 2f + 1 that has 3f + 1 number of nodes where f is the number of faulty nodes. For example, if a system has seven nodes and two of them are faulty then 5 nodes must agree.

### 5.15.5. Practical Byzantine Fault Tolerance (PBFT)

A solution to the byzantine general problem is the federated byzantine agreement. In this approach every node knows each other and knows which one is important and which is not [112]. PBFT is an algorithm which uses this approach. Hyperledger uses this principle and its consensus algorithm. The approach is like multicasting. A primary node is responsible to send requests to other nodes in its group. The service is said to be approved if 1/3 different replicas (nodes in the group) approves the receipt of the requests. If the client does not receive any replicas it will send requests to all the nodes instead of sending it to the primary only. This would be the case if the primary is faulty [113].

### 5.15.6. Raft

Raft can accommodate 50% of malicious nodes [114]. It is a voting-based consensus algorithm which is composed of two stages: leader election and log replication [115]. The ordering of transactions is a task given to the leader. When an existing leader fails, a randomized timeout for each server selects another leader. This way a leader is chosen. After a leader is chosen a replication stage starts. In this stage, the leader makes its own version of transaction log by accepting log entries form clients and broadcasting these transactions. This method has low latency and high throughput. The performance and throughput is dependent on the leader node so if the leader node is infected the whole system will be destroyed. It is not appropriate for IoT because of its low security and restricted throughput.

### 5.15.7. Proof of Proof

The proof of proof consensus method is used by VeriBlock. This protocol allows other blockchains to take security from other blockchains using proof of work. This creates an ecosystem wherein security initiates on well-known blockchains like bitcoin and spreads to other blockchains. A new type of miner is introduced by proof of proof (Available: https://medium.com/coinmonks/blockchain-consensus-algorithms-an-early-days-overview-2973f0cf49c6 accessed on 14 December 2019) who presents the current states of the blockchain to another blockchain. He does this by periodically performing publications on the current state of the blockchain. These publications are referenced in the event of a potential blockchain reorganization. Proof of proof creates blocks by using local PoW, POS or low-hash rate etc.

### 5.15.8. Proof of Believability

This protocol is the replacement of PoW as PoW is an expensive mechanism to adopt in every blockchain. Proof of Believability (Available: https://www.btcwires.com/round-the-block/what-is-proof-of-believability/ accessed on 3 December 2019) is developed by IOST (Internet of Service Token). A node is trusted based on its previous contributions. A token named SERVI is used in the IOST system to improve fairness and decentralization of the blockchain. Tokens are awarded to the good actors in order to select the next validator. Each node in proof of believability (PoB) has a believability score based on previous transactions of the node, number of positive reviews of a node, IOST's amount in the node and number of awarded SERVI.

### 5.15.9. Proof of Property

This proof allows participants not to have a local copy of the full blockchain [116]. Owner of new transaction should have coins enough in their address to fulfil the transaction. New participants can validate the transactions without the need to download a blockchain initially. The new participants need to access the root hash of the Patricia tree system state of the new block. As members of the network can obtain a state from the header so they can delete the old body of the blocks and save a lot of local space which is not the case in traditional blockchain applications.

## 6. Development Platforms

Now we discuss the development platforms used by the consensus algorithms. Table 5 describes some of the important features of the development environments.

**Table 5.** Comparison of blockchain technologies.

| Comparison Parameters | Ethereum | Cosmos | Cardano | EOS | Bitcoin | Hyperledger | Corda |
|---|---|---|---|---|---|---|---|
| Token | ETH | ATOM | ADA | EOS | Bitcoin | n/a | SDK |
| Public/Private | Public | Public/Private | Public | Public/Private | Public | Public/Private | Private |
| Programming Languages | Solidity | Java, C++, Python, Go | Haskell | JavaScript, Python, Ruby | Golang | Java, Golang, Node | Kotlin, Java |
| Consensus Algorithms | Proof of Work (Currently used), Proof of Stake (In Future) | Tendermint (Byzantine Fault-Tolerant, Proof of Stake) | Proof of Stack | Delegated Proof of Stack | Proof of Work | Practical Byzantine Fault Tolerance | Pluggable Consensus |
| Transactions Per Second | 25 | 10,000 | n/a | Millions (theoretically) | 1/3 to 1/7 | More than 1000 | Between 15 and 1678 TPS |
| Transaction Size | 1 MB | 250 bytes | n/a | n/a | 1 MB | Changeable (depending on framework) | Maximum size in bytes |
| Open Source | True | True | True | True | True | True | True |
| Pros | Anyone can write smart-contract and anyone can view that contract | Works like a hub for blockchains, based on Tendermint | Scalability, Side chain which reduce the risk of hacks. | Parallel processing, low latency, free usage (claimed not proven). | Safe and secure, High token value. | Don't use cryptocurrency so it is ideal for business networks. | Designed specifically for financial applications |
| Cons | Scalability issue, 25 transactions per second is very slow | Complex technology which may have compatibility issues with latest technologies and new blockchains | Maintaining side chain is complicated and it will require its own miners. | Never actually free, not fully decentralized, the free transaction fee are imposed on everyone who have EOS. | Very slow, not ideal for programming while there are other faster technologies. | There are a lot of frameworks to choose from and they all have different requirements to implement and setup. | Partially decentralized, not much suitable for IoT resource constrained networks |

### *6.1. Ethereum*

Ethereum is a crypto currency-based blockchain platform. It allows programmers to write smart contracts [117] which are self-executing methods. The language used for smart contracts writing is solidity. These smart contracts are executed by the Ethereum virtual machine (EVM). Every Ethereum node must have an EVM which keeps the copy of the blockchain. The EVM uses a stack register of 256-bits which is designed to run the same code as expected. EVM is also referred to as Ethereum yellow paper and it has been implemented in C++, Golang, Java, JavaScript, Ruby, Python and many others.

### *6.2. Cosmos*

Cosmos is also called the internet of blockchains, which actually is network for parallel blockchains. Before the idea of cosmos, blockchains were separated and isolated. Cosmos makes it easier for developers to build blockchains which can do transactions with each other. The end goal is the decentralized network of blockchains which is also referred to as "blockchain 3.0". It is open source and the Software Development Kit (SDK) is available online (Available: https://github.com/cosmos/sdk-application-tutorial, accessed on 20 January 2020). Currently the SDK is written in Golang but the cosmos team is open for changes. There are two other frameworks of cosmos technology which are Ethermint (Available: https://ethermint.zone/ accessed on 27 January 2020) and Lotion (Available: https://lotionjs.com/ accessed on 27 January 2020). Ethermint provides functionality like standard Ethereum including all the smart contract and EVM the only difference is that Ethermint uses PoS instead of PoW. Lotion is a javascript based tendermint consensus through which developers can make blockchains on the Cosmos network.

### *6.3. Cardano*

Cardano is a blockchain technology which allows the development of smart contract platforms. Cardano is made in Haskell programming language and it uses Plutus for smart contracts so both of programming languages are functional programming languages. For decentralized architecture the RINA (Recursive InterNetwork Architecture) network protocol is used for better bandwidth. In Cardano a node does not have the entire blockchain it uses pruning and partitioning but it is not fully implemented yet.

### *6.4. Electro-Optical System (EOS)*

EOS is a crypto currency powered by the EOSIO protocol [118]. This platform supports decentralized applications hosting decentralized storage and smart contracts. It uses the delegated proof of stake and is capable of running multithreaded which solves the issue of scalability better than most technologies. The main aim of EOSIO is to be a decentralized operating system which will allow developers to build decentralized applications such as steemit (Available: https://steemit.com/ accessed on 7 February 2020). The token EOS provides storage and bandwidth of the network so the percentage of EOS owned shows the percentage of bandwidth available to the owner. At present only 21 block producers are allowed who can generate blocks in 500 ms.

### *6.5. Bitcoin*

Bitcoin is the first cryptocurrency platform and it has the most expensive cryptocurrency. It has a public distributed ledger (the main blockchain) which keeps records of all the transactions of bitcoin currency. Those transactions are verified through cryptography and this cryptography is done by nodes called miners. The miner which solves the cryptographic puzzle first gains a reward in the form of cryptocurrency. In order to solve the cryptographic puzzle first, some miners join together to create a mining pool [119].

Bitcoin is solely a cryptocurrency platform, it also offers documentation (Available: https://bitcoin.org/en/developer-documentation accessed on 18 April 2020) for development but those are focused on wallets managing. It is not as flexible as other platforms, and it does not have any smart contract features or any application platform support.

### *6.6. Hyperledger*

The hyperledger block chain technology is out of the box unlike others. It does not have any cryptocurrency, it is just a technology which allows developers to build a whole new blockchain [120]. It is hosted by the Linux foundation designed to build private blockchains [121]. There are many frameworks and tools for hyperledger which are given in the Figure 15.

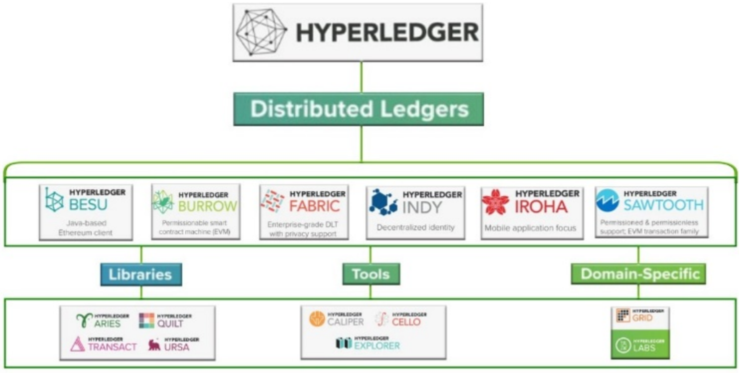

**Figure 15.** Hyperledger.

### *6.7. Corda*

Traditional blockchains may not be appropriate for many financial scenarios [122]. Corda provides the platform for smart contracts with some salient features i.e., this records and manages financial agreements between parties with compatibility of existing constructs. It supports several consensus mechanisms. Corda supports regulatory observer nodes. It allows access of data to only privileged ones [123]. The languages it supports are Kotlin and Java [124].

## **7. Blockchain Challenges**

In the following subsection, we discuss blockchain challenges. Although blockchain has improved a lot of applications and has a fault tolerant peer-to-peer network but blockchain always comes up with its vulnerabilities. We discuss the possible attacks on a blockchain ledger.

### *7.1. Denial of Service (DoS) Attacks*

The attacker crash a node by flooding a large amount of traffic in a denial of service (DoS) [125]. It prevents authorized users from retrieving the service or resource. Similarly, a distributed denial of service (DDoS) is another type of attack where a node is flooded with malevolent requests. In DDoS multiple attackers attack a single node.

### *7.2. Sybil Attacks*

Multiple identities attacking a larger portion of network is called a sybil attack. The invaders can launch numerous false nodes that seem to be honest to their peers. These false nodes take part in falsifying the network to authenticate illegal transactions and to modify valid transactions. They can use virtual machines, several devices, or internet protocol (IP) addresses as bogus nodes for the attack. The peer to peer (P2P) network assumes that every participating node contains only one identity. Thus, numerous forged nodes give attackers the ability to repudiate transmitted blocks and to outvote authentic nodes. When an attacker controls a large number of nodes in the network, it increases the chances of double-spending [126].

### *7.3. Eclipse Attacks*

In an eclipse attack [127], specific nodes are isolated from the peer-to-peer network by the attacker. Similar to sybil attacks, it does not attack the entire network. Once the target node is isolated, the attacker controls all outgoing connections of the node [128]. From there on, the attacker can abuse the target network and dispatch distinctive sorts of attack on blockchain mining power and agreement components. These attacks include double spending, engineering block races, selfish mining and splitting mining power.

### *7.4. Routing Attacks*

In routing attacks [129], a message is intercepted by the attacker in the blockchain network. The attack alters the message and sends it to its neighbors. Furthermore, this attack is divided into a partitioning attack and delay attack. In partitioning attack, the entire blockchain network is divided into two or more portions. In a delayed attack, the attacker captures the message and tampers with it. Then, it redirects the tamper message to another blockchain network portion.

Different consensus mechanisms are used by blockchain to develop trust among blockchain peers. However, there are some possible attacks on these consensus mechanisms.

### *7.5. The 51% Attacks*

A miner, having 51% or more hashing power, can initiate a 51% attack in the blockchain network [130]. The 51% attack, enables the attacker to stop the confirmation of a new block. Additionally, the attacker can reverse transactions already confirmed by the blockchain.

### *7.6. Double Spending*

In double spending multiple transactions with the same cryptocurrency are performed by a user [131,132]. This transaction is broadcast to each node in that network. This transaction needs to be confirmed by the nodes, this confirmation is time consumable [131]. This time between two transactions' initiation and confirmation can be a window for the attacker to quickly launch his/her attack [133,134].

### *7.7. Alternative History Attacks*

In alternative history attack, a transaction is sent to the merchant by the attacker [135,136]. In addition, a double spending transaction is included by the attacker in an alternative blockchain fork [137,138]. The merchant sends the product after n blocks confirmation. Therefore, the attacker tries to find more than n blocks. If the attacker succeeds, he gains his coins by releasing the fork.

### *7.8. Race Attacks*

In the race attack, the attacker creates two transactions. The first transaction is sent to the merchant by the attacker [139,140]. This product is sent by the merchant without confirmation. Meanwhile, the second transaction is broadcast by the attacker to invalidate the first transaction.

### *7.9. Finney Attack*

In the finney attack [141], two similar transactions i.e., one crediting the target and the other crediting the attacker are used by the attacker [142,143]. This attack mines a block which including the first transaction and delays publishing it. Meanwhile, the attacker mines the second transaction. When the attacker succeeds, he purchases goods with the first transaction. Then, he releases the pre-mined block which includes the first transaction. The attacker receives both goods and coins whereas the merchant finds their transaction invalid [144,145].

## **8. Blockchain Research Issues**

We discuss blockchain research issues of different applications in this section.

### *8.1. Blockchain-Based Research Issues in Healthcare*

Blockchain has improved the medical and smartphone applications but there are still some security issues as blockchain comes with potential problems. Any industry including healthcare that needs to use blockchain and its devices should train themselves in these areas to improve it. Such an education can improve patient-centered data [146,147]. The blockchain experiments in this research needs a patient to authorize himself before transferring a record and this could lead to threats. Key leakage and management is another issue that is not addressed. If a key is lost by a patient the data is difficult or impossible to be authenticated or recovered. A mechanism should be discovered for recovering data. Traditional blockchain cannot be enough in the case of large amount of patient's storage and sharing data so a double blockchain solution is presented by Lejun Zhang [148].

### *8.2. Blockchain-Based Research Issues/Future Work in Intelligent Transportation System (ITS) and Internet of Things (IoT)*

An ITS aims to improve road safety and traffic management [149,150]. Vehicles share the information regarding their position, speed and direction etc. with other vehicles [151,152] as they carry sensing data via dedicated short range communication [153]. In ITS, nodes can communicate with each other via different blockchain apps at a large scale autonomously forming decentralized autonomous organizations (DAOs) or decentralized autonomous systems (DASs). Research is needed into the microscopic level of these autonomous agents. A concrete work is also needed in system modeling of self-adaptive, self-evolving and self-organizing DAO and DASs. Moreover, mechanisms should be designed for crowd-sourcing incentives. There are more interesting issues in ITS such as credit evaluation of ITS assets and trust-based management which needs more efforts of research. Further study needs to be undertaken in smart contract-based ITS and data security and privacy issues to prevent the easier 51% attack in ITS. Blockchain can be explored more to incorporate with IoT [154] for improving security and privacy in various domains of smart application [155]. G. Ali [156] suggested a blockchain-based framework for access delegation in IoT which produces high throughput in the case of a large number of concurrent requests. Therefore, further investigation needs to be undertaken in such scenarios.

### *8.3. Blockhain Research Issues/Future Work in Real Estate*

Private blockchain using smart contracts can be a best solution for recording transactions of real estate having high transaction fees [157]. Using resource information by a customer can lead to a conclusion about the business work of other customers. So a hybrid blockchain which includes both private and public best features can be deployed to audit the access of data as it provides the most authoritative system for the participating nodes [158].

## 9. Conclusions and Future Work

The paper discusses blockchain, its architecture and blockchain applications. The categorization of this paper provides an insight into blockchain technology along with its applications in different areas. We provide extensive knowledge on consensus methods used in not only cryptocurrencies but also in other areas like healthcare, intelligent transportation systems, supply chains, banks, education, and other areas. The consensuses discussed relate to permissioned as well as permissionless, private and public. This paper contributes to helping identify which algorithm should be used in which particular scenario. The paper has also explored some of the development platforms where re- searchers can get a benefit of using them according to their work needs. This survey also highlights some of the blockchain research issues in different applications as well as some common attacks. In future, studies can explore more consensus algorithms as in IoT, machine learning, intelligent transportation systems etc. Applications are not specific to those mentioned in this paper so more applications can be explored and added. Open blockchain-based research issues in academic subjects like software engineering, databases and networks etc must be considered.

**Author Contributions:** Conceptualization, S.J. and N.A. Writing—original draft, S.J.; Project Administration, N.A.; writing—review and editing, W.A. and A.D.; funding acquisition, H.C. resources. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research project was funded by Higher Education Commission (HEC) "Provable Security of Blockchain under National Centre for Cyber Security (NCCS), University of Peshawar (UOP)".

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** No reported data.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Velde, F. *Bitcoin: A Primer*; Essays on Issues the Federal Reserve Bank of Chicago Dec; Federal Reserve Bank of Chicago: Chicago, IL, USA, 2013.
2. Shoker, A. Sustainable blockchain through proof of exercise. In Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–9.
3. Brito, J.; Castillo, A. *Bitcoin: A Primer for Policymakers*; Mercatus Center at George Mason University: Fairfax, VA, USA, 2013.
4. Swan, M. Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]. *IEEE Technol. Soc. Mag.* **2015**, *34*, 41–52. [CrossRef]
5. Bahga, A.; Madisetti, V. *Blockchain Applications: A Hands-On Approach*; Vpt, 2017. Available online: Laportecountymealsonwheels.org (accessed on 6 October 2018).
6. El Ioini, N.; Pahl, C. A review of distributed ledger technologies. In *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*; Springer: Cham, Switzerland, 2018; pp. 277–288.
7. Anceaume, E.; Guellier, A.; Ludinard, R.; Sericola, B. Sycomore: A permissionless distributed ledger that self-adapts to transactions demand. In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 1–3 November 2018; pp. 1–8.
8. Hughes, A.; Park, A.; Kietzmann, J.; Archer-Brown, C. Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. *Bus. Horiz.* **2019**, *62*, 273–281. [CrossRef]
9. Rizal Batubara, F.; Ubacht, J.; Janssen, M. Unraveling Transparency and Accountability in Blockchain. In Proceedings of the 20th Annual International Conference on Digital Government Research, Dubai, United Arab Emirates, 18–20 June 2019; pp. 204–213.
10. Karame, G. On the security and scalability of bitcoin's blockchain. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1861–1862.
11. Wattenhofer, R. *Distributed Ledger Technology: The Science of the Blockchain*; CreateSpace Independent, 2017. Available online: https://lib.hpu.edu.vn/handle/123456789/28113 (accessed on 8 May 2021).
12. Xu, X.; Weber, I.; Staples, M. *Architecture for Blockchain Applications*; Springer: Berlin/Heidelberg, Germany, 2019.
13. Puthal, D.; Malik, N.; Mohanty, S.P.; Kougianos, E.; Yang, C. The blockchain as a decentralized security framework [future directions]. *IEEE Consum. Electron. Mag.* **2018**, *7*, 18–21. [CrossRef]
14. Shahriar Hazari, S.; Mahmoud, Q.H. Improving Transaction Speed and Scalability of Blockchain Systems via Parallel Proof of Work. *Future Internet* **2020**, *12*, 125. [CrossRef]
15. Chatzigiannis, P.; Baldimtsi, F.; Griva, I.; Li, J. Diversification across mining pools: Optimal mining strategies under pow. *arXiv* **2019**, arXiv:1905.04624.
16. Hofmann, F.; Wurster, S.; Ron, E.; Böhmecke-Schwafert, M. The immutability concept of blockchains and benefits of early standardization. In Proceedings of the 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), Nanjing, China, 27–29 November 2017; pp. 1–8.
17. Landerreche, E.; Stevens, M. On immutability of blockchains. In Proceedings of the 1st ERCIM Blockchain Workshop 2018, Amsterdam, The Netherlands, 8–9 May 2018; European Society for Socially Embedded Technologies (EUSSET): Zurich, Switzerland, 2018.
18. Aste, T.; Tasca, P.; Di Matteo, T. Blockchain technologies: The foreseeable impact on society and industry. *Computer* **2017**, *50*, 18–28. [CrossRef]
19. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptographyand privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
20. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 1–36.

21. Bach, L.; Mihaljevic, B.; Zagar, M. Comparative analysis of blockchain consensus algorithms. In Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; pp. 1545–1550.
22. Chalaemwongwan, N.; Kurutach, W. State of the art and challenges facing consensus protocols on blockchain. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 957–962.
23. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
24. Nguyen, G.T.; Kim, K. A Survey about Consensus Algorithms Used in Blockchain. *J. Inf. Process. Syst.* **2018**, *14*, 101–128.
25. Chaudhry, N.; Yousaf, M.M. Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities. In Proceedings of the 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan, 19–21 December 2018; pp. 54–63.
26. Zhao, W.; Yang, S.; Luo, X. On consensus in public blockchains. In Proceedings of the 2019 International Conference on Blockchain Technology, Honolulu, HI, USA, 15–18 March 2019; pp. 1–5.
27. Aras, S.T.; Kulkarni, V. Blockchain and Its Applications–A Detailed Survey. *Int. J. Comput. Appl.* **2017**, *180*, 29–35.
28. Mohan, C. State of public and private blockchains: Myths and reality. In Proceedings of the 2019 International Conference on Management of Data, Amsterdam, The Netherlands, 30 June–5 July 2019; pp. 404–411.
29. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
30. Sagirlar, G.; Carminati, B.; Ferrari, E.; Sheehan, J.D.; Ragnoli, E. Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1007–1016.
31. Manian, Z.N.; Krishnan, R.; Sriram, S. Hybrid Blockchain. U.S. Patent 20,170,243,193A1, 24 August 2017.
32. Ranade, A.; Shaikh, Z. A Survey on Blockchain Technology with Use-Cases in Governance. 2020. Available online: https://papers.ssrn.com/SSRN3568629 (accessed on 20 April 2020).
33. Zhu, S.; Cai, Z.; Hu, H.; Li, Y.; Li, W. zkCrowd: A hybrid blockchain-based crowdsourcing platform. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4196–4205. [CrossRef]
34. Sun, J.; Yan, J.; Zhang, K.Z. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financ. Innov.* **2016**, *2*, 26. [CrossRef]
35. Lee, J.H. BIDaaS: Blockchain based ID as a service. *IEEE Access* **2017**, *6*, 2274–2278. [CrossRef]
36. Hassani, H.; Huang, X.; Silva, E. Big-crypto: Big data, blockchain and cryptocurrency. *Big Data Cogn. Comput.* **2018**, *2*, 34. [CrossRef]
37. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
38. Pavlov, E.; Rosenschein, J.S.; Topol, Z. Supporting privacy in decentralized additive reputation systems. In Proceedings of the International Conference on Trust Management, Oxford, UK, 29 March–1 April 2004; Springer: Berlin/Heidelberg, Germany, 2004; pp. 108–119.
39. Hasan, O.; Brunie, L.; Bertino, E. Preserving privacy of feedback providers in decentralized reputation systems. *Comput. Secur.* **2012**, *31*, 816–826. [CrossRef]
40. Sharples, M.; Domingue, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In Proceedings of the European Conference on Technology Enhanced Learning, Lyon, France, 13–16 September 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 490–496.
41. Albeanu, G. Blockchain technology and education. In Proceedings of the 12th International Conference on Virtual Learning ICVL, Sibiu, Romania, 28 October 2017; pp. 271–275.
42. Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-based applications in education: A systematic review. *Appl. Sci.* **2019**, *9*, 2400. [CrossRef]
43. Turkanović, M.; Hölbl, M.; Košič, K.; Heričko, M.; Kamišalić, A. EduCTX: A blockchain-based higher education credit platform. *IEEE Access* **2018**, *6*, 5112–5127. [CrossRef]
44. Sestoft, P. Autonomous Pension Funds on the Blockchain; 1998 ACM Subject Classification, Report from Dagstuhl Seminar 17132, 26–29 March 2017. Available online: http://www.dagstuhl.de/17132 (accessed on 20 April 2019).
45. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Appl. Sci.* **2019**, *9*, 1736. [CrossRef]
46. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
47. Khan, M.A.; Algarni, F.; Quasim, M.T. Decentralised Internet of Things. In *Decentralised Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 3–20.
48. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]

49. Parker, D. Blockchain Voting Used By Danish Political Party. *CryptoCoinsNews*. 23 April 2014. Available online: https://www.ccn.com/blockchain-voting-used-by-danish-political-party (accessed on 15 September 2019).
50. Saroop, S. *Block chain Technology: Assessment from Application Perspectives*; Technical Report; University of Manchester EasyChair: Manchester, UK, 2020.
51. Hjálmarsson, F.Þ.; Hreiðarsson, G.K.; Hamdaqa, M.; Hjálmtýsson, G. Blockchain-based e-voting system. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 983–986.
52. Brophy, R. Blockchain and insurance: A review for operations and regulation. *J. Financ. Regul. Compliance* **2019**, *28*, 215–234. [CrossRef]
53. Raikwar, M.; Mazumdar, S.; Ruj, S.; Gupta, S.S.; Chattopadhyay, A.; Lam, K.Y. A blockchain framework for insurance processes. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–4.
54. Ibba, S.; Pinna, A.; Seu, M.; Pani, F.E. CitySense: Blockchain-oriented smart cities. In Proceedings of the XP2017 Scientific Workshops, Cologne, Germany, 22–26 May 2017; pp. 1–5.
55. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
56. Ali, G.; Ahmad, N.; Cao, Y.; Asif, M.; Cruickshank, H.; Ali, Q.E. Blockchain based permission delegation and access control in Internet of Things (BACI). *Comput. Secur.* **2019**, *86*, 318–334. [CrossRef]
57. Ali, G.; Ahmad, N.; Cao, Y.; Ali, Q.E.; Azim, F.; Cruickshank, H. BCON: Blockchain based access CONtrol across multiple conflict of interest domains. *J. Netw. Comput. Appl.* **2019**, *147*, 102440. [CrossRef]
58. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
59. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
60. Chakravorty, A.; Rong, C. Ushare: User controlled social media based on blockchain. In Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication, Beppu, Japan, 5–7 January 2017; p. 99.
61. Basden, J.; Cottrell, M. How utilities are using blockchain to modernize the grid. *Harv. Bus. Rev.* **2017**, *23*, 1–8.
62. Syed, T.A.; Alzahrani, A.; Jan, S.; Siddiqui, M.S.; Nadeem, A.; Alghamdi, T. A comparative analysis of blockchain architecture and its applications: Problems and recommendations. *IEEE Access* **2019**, *7*, 176838–176869. [CrossRef]
63. Golosova, J.; Romanovs, A. Overview of the blockchain technology cases. In Proceedings of the 2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), Riga, Latvia, 10–12 October 2018; pp. 1–6.
64. Nofer, M.; Gomber, P.; Hinz, O.; Schiereck, D. Blockchain. *Bus. Inf. Syst. Eng.* **2017**, *59*, 183–187. [CrossRef]
65. Beck, R. Beyond bitcoin: The rise of blockchain world. *Computer* **2018**, *51*, 54–58. [CrossRef]
66. Lucas, B.; Páez, R.V. Consensus Algorithm for a Private Blockchain. In Proceedings of the 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 12–14 July 2019; pp. 264–271.
67. Gramoli, V. From blockchain consensus back to byzantine consensus. *Future Gener. Comput. Syst.* **2020**, *107*, 760–769. [CrossRef]
68. Nakamoto, S.; Bitcoin, A. A Peer-to-Peer Electronic Cash System. Bitcoin. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 20 June 2019).
69. Osadchuk, M.; Oliynykov, R. Method of Proof of Work consensus algorithms comparison. *Радиотехника* **2019**, *198*, 105–112. [CrossRef]
70. Larimer, D. Delegated proof-of-stake (dpos). *Bitshare Whitepaper* **2014**, *81*, 85.
71. Wahab, A.; Mehmood, W. Survey of consensus protocols. *arXiv* **2018**, arXiv:1810.03357.
72. Abraham, I.; Malkhi, D. The blockchain consensus layer and BFT. *Bull. EATCS* **2017**, *3*, 2017.
73. Kotilevets; Ivanova, I.; Romanov, I.; Magomedov, S.; Nikonov, V.; Pavelev, S. Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions. *IFAC-PapersOnLine* **2018**, *51*, 693–696. [CrossRef]
74. Muratov, F.; Lebedev, A.; Iushkevich, N.; Nasrulin, B.; Takemiya, M. YAC: BFT consensus algorithm for blockchain. *arXiv* **2018**, arXiv:1809.00554.
75. Bamakan, S.M.H.; Motavali, A.; Bondarti, A.B. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, *154*, 113385. [CrossRef]
76. Zhang, S.; Lee, J.H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2020**, *6*, 93–97. [CrossRef]
77. Milutinovic, M.; He, W.; Wu, H.; Kanwal, M. Proof of luck: An efficient blockchain consensus protocol. In Proceedings of the 1st Workshop on System Software for Trusted Execution, Trento, Italy, 12–16 December 2016; p. 2.
78. Miller, A.; Juels, A.; Shi, E.; Parno, B.; Katz, J. Permacoin: Repurposing bitcoin work for data preservation. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 475–490.
79. Corso, A. Performance Analysis of Proof-Of-Elapsed-Time (POET) Consensus in the Sawtooth Blockchain Framework. Master's Thesis, University of Oregon, Eugene, OR, USA, 2019.
80. Crosby, M.; Nachiappan; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyondbitcoin. *Appl. Innov.* **2016**, *2*, 71.

81. De Angelis, S.; Aniello, L.; Baldoni, R.; Lombardi, F.; Margheri, A.; Sassone, V. Pbft vs proof-of- authority: Applying the cap theorem to permissioned blockchain. In Proceedings of the Second Italian Conference on Cyber Security, Milan, Italy, 6–9 February 2018.
82. Ferdous, M.S.; Chowdhury, M.J.M.; Hoque, M.A.; Colman, A. Blockchain Consensuses Algorithms: A Survey. *arXiv* **2020**, arXiv:2001.07091.
83. Macdonald, M.; Liu-Thorrold, L.; Julien, R. The blockchain: A comparison of platforms and their uses beyond bitcoin. In Proceedings of the COMS4507-Adv. Computer and Network Security, The University of Queensland, Brisbane, Australia, 30 May 2017; Work Pap; pp. 1–18.
84. Ren, L. Proof of Stake Velocity: Building the Social Currency of the Digital Age. *Self-Publ. White Paper*. 2014. Available online: https://www.semanticscholar.org/paper/Proof-of-Stake-Velocity%3A-Building-the-Social-of-the-Ren/8499c0b3d1138200fdebb88f964100d54a531878 (accessed on 6 July 2021).
85. Moran, T.; Orlov, I. Proofs of Space-Time and Rational Proofs of Storage. *IACR Cryptol. ePrint Arch.* **2016**, *2016*, 35.
86. Innerbichler, J.; Damjanovic-Behrendt, V. Federated byzantine agreement to ensure trustworthiness of digital manufacturing platforms. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 15 June 2018; pp. 111–116.
87. Peterson, K.; Deeduvanu, R.; Kanjamala, P.; Boles, K. A blockchain-based approach to health information exchange networks. *Proc. NIST Workshop Blockchain Healthc.* **2016**, *1*, 1–10.
88. Kumar, M.; Chand, S. MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic. *J. Netw. Comput. Appl.* **2021**, *179*, 102975. [CrossRef] [PubMed]
89. Talukder, A.K.; Chaitanya, M.; Arnold, D.; Sakurai, K. Proof of disease: A blockchain consensus protocol for accurate medical decisions and reducing the disease burden. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 8–12 October 2018; pp. 257–262.
90. Chen, J.; Ma, X.; Du, M.; Wang, Z. A Blockchain Application for Medical Information Sharing. In Proceedings of the 2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE), Beijing, China, 30 March–1 April 2018; pp. 1–7.
91. Singh, M.; Kim, S. Blockchain based intelligent vehicle data sharing framework. *arXiv* **2017**, arXiv:1708.09721.
92. Yuan, Y.; Wang, F.Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2663–2668.
93. Yang, Z.; Zheng, K.; Yang, K.; Leung, V.C. A blockchain-based reputation system for data credibility assessment in vehicular networks. In Proceedings of the 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
94. Kamilaris, A.; Fonts, A.; Prenafeta-Boldύ, F.X. The rise of blockchain technology in agriculture and food supply chains. *Trends Food Sci. Technol.* **2019**, *91*, 640–652. [CrossRef]
95. Singh, R.; Benyoucef, L. A consensus based group decision making methodology for strategic selection problems of supply chain coordination. *Eng. Appl. Artif. Intell.* **2013**, *26*, 122–134. [CrossRef]
96. Leng, K.; Bi, Y.; Jing, L.; Fu, H.C.; Van Nieuwenhuyse, I. Research on agricultural supply chain system with double chain architecture based on blockchain technology. *Future Gener. Comput. Syst.* **2018**, *86*, 641–649. [CrossRef]
97. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
98. Aileni, R.M.; Suciu, G. IoMT: A blockchain perspective. In *Decentralised Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 199–215.
99. Li, S.; Oikonomou, G.; Tryfonas, T.; Chen, T.M.; Da Xu, L. A distributed consensus algorithm for decision making in service-oriented internet of things. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1461–1468.
100. Yang, C.; Li, X.; Yu, Y.; Wang, Z. Basing Diversified Services of Complex IIoT Applications on Scalable Block Graph Platform. *IEEE Access* **2019**, *7*, 22966–22975. [CrossRef]
101. Lamport, L. Paxos made simple. *ACM Sigact News* **2001**, *32*, 18–25.
102. Brambilla, G.; Amoretti, M.; Zanichelli, F. Using blockchain for peer-to-peer proof-of-location. *arXiv* **2016**, arXiv:1607.00174.
103. Fu, D.; Fang, L. Blockchain-based trusted computing in social network. In Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 14–17 October 2016; pp. 19–22.
104. O'Dair, M.; Beaven, Z.; Neilson, D.; Osborne, R.; Pacifico, P. Music On The Blockchain: Blockchain For Creative Industries Research Cluster. *Middx. Univ. Rep.* **2016**, *1*, 4–24.
105. Spielman, A. Blockchain: Digitally Rebuilding the Real Estate Industry. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2016.
106. Foroglou, G.; Tsilidou, A.L. Further applications of the blockchain. In Proceedings of the 12th Student Conference on Managerial Science and Technology, Athens, Greece, 14 May 2015.
107. Baum, A. PropTech 3.0: The Future of Real Estate. 2017. Available online: https://www.sbs.ox.ac.uk/sites/default/files/2018-07/PropTech3.0.pdf (accessed on 20 May 2020).

108. Guan, Z.; Si, G.; Zhang, X.; Wu, L.; Guizani, N.; Du, X.; Ma, Y. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. *IEEE Commun. Mag.* **2018**, *56*, 82–88. [CrossRef]
109. Chen, Y. Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain. In Proceedings of the 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Bangkok, Thailand, 18–20 December 2017; pp. 466–473.
110. Buchman, E. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. Ph.D. Thesis, University of Guelph School of Engineering, Guelph, ON, Canada, 2016.
111. Blocki, J.; Zhou, H.S. Designing proof of human-work puzzles for cryptocurrency and beyond. In *Theory of Cryptography Conference*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 517–546.
112. Namasudra, S.; Deka, G.C.; Johri, P.; Hosseinpour, M.; Gandomi, A.H. The revolution of blockchain: State-of-the-art and research challenges. *Arch. Comput. Methods Eng.* **2020**, *28*, 1497–1515. [CrossRef]
113. Castro, M.; Liskov, B. Practical byzantine fault tolerance. *OSDI* **1999**, *99*, 173–186.
114. Castro, M.; Liskov, B. Practical Byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst.* **2002**, *20*, 398–461. [CrossRef]
115. Ongaro, D.; Ousterhout, J. *The Raft Consensus Algorithm*; Stanford University: Stanford, CA, USA, 2015.
116. Huang, D.; Ma, X.; Zhang, S. Performance analysis of the Raft consensus algorithm for private blockchains. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *50*, 172–181. [CrossRef]
117. Ehmke, C.; Wessling, F.; Friedrich, C.M. Proof-of-property: A lightweight and scalable blockchain protocol. In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, Gothenburg, Sweden, 27 May–3 June 2018; pp. 48–51.
118. Dannen, C. Solidity programming. In *Introducing Ethereum and Solidity*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 69–88.
119. IO, E. EOS. IO Technical White Paper. EOS. IO. Available online: https://github.com/EOSIO/Documentation2017 (accessed on 18 December 2017).
120. Lewenberg, Y.; Bachrach, Y.; Sompolinsky, Y.; Zohar, A.; Rosenschein, J.S. Bitcoin mining pools: A cooperative game theoretic analysis. In Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, Istanbul, Turkey, 4–8 May 2015; pp. 919–927.
121. Cachin, C. Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*; IBM Research—Zurich CH-8803: Ruschlikon, Switzerland, 2016; Volume 310.
122. Dhillon, V.; Metcalf, D.; Hooper, M. The hyperledger project. In *Blockchain Enabled Applications*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 139–149.
123. Valenta, M.; Sandner, P. Comparison of ethereum, hyperledger fabric and corda. *Frankf. Sch. Blockchain Cent.* **2017**, *8*, 1–8.
124. Brown, R.G.; Carlyle, J.; Grigg, I.; Hearn, M. Corda: An introduction. *R3 CEV* **2016**, *1*, 15.
125. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling blockchain: A data processing view of blockchain systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]
126. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
127. Sayeed, S.; Marco-Gisbert, H. Assessing blockchain consensus and security mechanisms against the 51% attack. *Appl. Sci.* **2019**, *9*, 1788. [CrossRef]
128. Wüst, K.; Gervais, A. *Ethereum Eclipse Attacks*; Technical Report; ETH: Zurich, Germany, 2016.
129. Nayak, K.; Kumar, S.; Miller, A.; Shi, E. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbruecken, Germany, 21–24 March 2016; pp. 305–320.
130. Sahay, R.; Geethakumari, G.; Mitra, B. A novel blockchain based framework to secure IoT-LLNs against routing attacks. *Computing* **2020**, *102*, 2445–2470. [CrossRef]
131. Saad, M.; Cook, V.; Nguyen, L.; Thai, M.T.; Mohaisen, A. Partitioning attacks on bitcoin: Colliding space, time, and logic. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1175–1187.
132. Natoli, C.; Gramoli, V. The blockchain anomaly. In Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 31 October–2 November 2016; pp. 310–317.
133. Pilkington, M. Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK, 2016. Available online: https://www.elgaronline.com/ (accessed on 16 May 2021).
134. Lee, H.; Shin, M.; Kim, K.S.; Kang, Y.; Kim, J. Recipient-oriented transaction for preventing double spending attacks in private blockchain. In Proceedings of the 2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Hong Kong, China, 11–13 June 2018; pp. 1–2.
135. Rosenfeld, M. Analysis of hashrate-based double spending. *arXiv* **2014**, arXiv:1402.2009.
136. Pérez-Solà, C.; Delgado-Segura, S.; Navarro-Arribas, G.; Herrera-Joancomartí, J. Double-spending prevention for bitcoin zero-confirmation transactions. *Int. J. Inf. Secur.* **2019**, *18*, 451–463. [CrossRef]

137. Malik, A.; Gautam, S.; Abidin, S.; Bhushan, B. Blockchain Technology-Future of IoT: Including Structure, Limitations and Various Possible Attacks. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019; Volume 1, pp. 1100–1104.
138. Mechkaroska, D.; Dimitrova, V.; Popovska-Mitrovikj, A. Analysis of the possibilities for improvement of BlockChain technology. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR) IEEE, Belgrade, Serbia, 20–21 November 2018; pp. 1–4.
139. Morganti, G.; Schiavone, E.; Bondavalli, A. Risk Assessment of Blockchain Technology. In Proceedings of the 2018 Eighth Latin-American Symposium on Dependable Computing (LADC), Belgrade, Serbia, 20–21 November 2018; pp. 87–96.
140. Alkhalifah, A.; Ng, A.; Kayes, A.; Chowdhury, J.; Alazab, M.; Watters, P.A. A taxonomy of blockchain threats and vulnerabilities. In *Blockchain for Cybersecurity and Privacy*; CRC Press: Boca Raton, FL, USA, 2020; pp. 3–28.
141. Dasgupta, D.; Shrein, J.M.; Gupta, K.D. A survey of blockchain from security perspective. *J. Bank. Financ. Technol.* **2019**, *3*, 1–17. [CrossRef]
142. Alizadeh, M.; Andersson, K.; Schelén, O. A Survey of Secure Internet of Things in Relation to Blockchain. *J. Internet Serv. Inf. Secur.* **2020**, *3*, 47–75.
143. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.; Mohaisen, A. Exploring the attack surface of blockchain: A systematic overview. *arXiv* **2019**, arXiv:1904.03487.
144. Kaushik, A.; Choudhary, A.; Ektare, C.; Thomas, D.; Akram, S. Blockchain—Literature survey. In Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017; pp. 2145–2148.
145. Vokerla, R.R.; Shanmugam, B.; Azam, S.; Karim, A.; De Boer, F.; Jonkman, M.; Faisal, F. An Overview of Blockchain Applications and Attacks. In Proceedings of the 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 30–31 March 2019; pp. 1–6.
146. McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
147. Lunardi, R.C.; Michelin, R.A.; Neu, C.V.; Nunes, H.C.; Zorzo, A.F.; Kanhere, S.S. Impact of consensus on appendable-block blockchain for IoT. In Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Houston, TX, USA, 12–14 November 2019; pp. 228–237.
148. Zhang, L.; Peng, M.; Wang, W.; Su, Y.; Cui, S.; Kim, S. Secure and Efficient Data Storage and Sharing Scheme Based on Double Blockchain. *CMC Comput. Mater. Contin.* **2021**, *66*, 499–515.
149. Ali, Q.E.; Ahmad, N.; Malik, A.H.; Ali, G.; Rehman, W.U. Issues, challenges, and research opportunities in intelligent transport system for security and privacy. *Appl. Sci.* **2018**, *8*, 1964. [CrossRef]
150. Ali, Q.E.; Ahmad, N.; Malik, A.H.; Rehman, W.U.; Din, A.U.; Ali, G. ASPA: Advanced Strong Pseudonym based Authentication in Intelligent Transport System. *PLoS ONE* **2019**, *14*, e0221213. [CrossRef]
151. Taleb, T.; Sakhaee, E.; Jamalipour, A.; Hashimoto, K.; Kato, N.; Nemoto, Y. A stable routing protocol to support ITS services in VANET networks. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3337–3347. [CrossRef]
152. Taleb, T.; Ochi, M.; Jamalipour, A.; Kato, N.; Nemoto, Y. An efficient vehicle-heading based routing protocol for VANET networks. In Proceedings of the IEEE Wireless Communications and Networking Conference, 2006, WCNC 2006, Las Vegas, NV, USA, 3–6 April 2006; Volume 4, pp. 2199–2204.
153. Qi, W.; Landfeldt, B.; Song, Q.; Guo, L.; Jamalipour, A. Traffic differentiated clustering routing in DSRC and C-V2X hybrid vehicular networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 7723–7734. [CrossRef]
154. Alghamdi, N.S.; Khan, M.A. Energy-Efficient and Blockchain-Enabled Model for Internet of Things (IoT) in Smart Cities. *CMC Comput. Mater. Contin.* **2021**, *66*, 2509–2524.
155. Alamri, M.; Jhanjhi, N.; Humayun, M. Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 244–258.
156. Gauhar, A.; Ahmad, N.; Cao, Y.; Khan, S.; Cruickshank, H.; Qazi, E.A.; Ali, A. xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things. *IEEE Access* **2020**, *8*, 58800–58816. [CrossRef]
157. Ahmad, I.; Alqarni, M.A.; Almazroi, A.A.; Alam, L. Real Estate Management via a Decentralized Blockchain Platform. *CMC Comput. Mater. Contin.* **2021**, *66*, 1813–1822.
158. Li, M.; Shen, L.; Huang, G.Q. Blockchain-enabled workflow operating system for logistics resources sharing in E-commerce logistics real estate service. *Comput. Ind. Eng.* **2019**, *135*, 950–969. [CrossRef]