Framework for Determining the Suitability of Blockchain: Criteria and Issues to Consider

Article *in* Transactions on Emerging Telecommunications Technologies · October 2021

DOI: 10.1002/ett.4334

6 authors, including:

Vikas Hassija
Jaypee Institute of Information Technology
45 PUBLICATIONS **1,563** CITATIONS
SEE PROFILE

Vinay Chamola
Birla Institute of Technology and Science Pilani
132 PUBLICATIONS **2,931** CITATIONS
SEE PROFILE

Shashank Gupta
Birla Institute of Technology and Science Pilani
66 PUBLICATIONS **932** CITATIONS
SEE PROFILE

Received 18 December 2020; | Revised 30 April June 2021, and 4 June 2021; | Accepted 8 July 2021

DOI: xxx/xxxx

ARTICLE TYPE

Framework for Determining the Suitability of Blockchain: Criteria and Issues to Consider

Vikas hassija[1] | Sherali Zeadally[2] | Ishan Jain[1] | Aman Tahiliani[1] | Vinay Chamola*[3] | Shashank Gupta[4]

[1]Department of CSE and IT, Jaypee Institute of Information Technology, UP, India
[2]College of Communication and Information, University of Kentucky, Lexington, USA
[3]Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus, India
[4]Department of Computer Science and Information Systems, BITS-Pilani, Pilani Campus, India

Correspondence
*Vinay Chamola Email: vinay.chamola@pilani.bits-pilani.ac.in

Summary

Various Distributed Ledger Technologies (DLTs), such as Blockchain, have evolved significantly in recent years. These technologies provide a robust and effective solution for providing confidentiality, integrity, non-repudiation, authentication and transparency. While Blockchain has many advantages, it has various limitations as well, such as complexity, low throughput, privacy, and so on. We discuss the issues that must be considered when deciding whether to use these technologies in a given case or not. We describe the operation of Blockchain, application areas where Blockchain is suitable, and those where it is not. We also discuss the applicability of other emerging DLTs, apart from blockchain technology, such as Hashgraph, Zcash, Nano coin, and IOTA.

KEYWORDS:
Blockchain, consensus algorithms, distributed ledger technologies, security, permission-less blockchain, permissioned blockchain, blockchain alternatives

1 | INTRODUCTION

As the name suggests, a Blockchain can be considered as a database where digital information (i.e. "Blocks") is stored in a distributed network as a chain of blocks. Blockchain falls in the class of Distributed Ledger Technologies (DLT) that allow a database to be used and maintained in a distributed manner. Blockchain provides a shared ledger of transactions[1] that can be read, verified and stored in the form of blocks, forming a chain-like structure. Depending on the size of the transaction, a block may store up to a few thousand transactions (e.g., a single block in the Bitcoin Blockchain can store about 1MB of data). The security and anonymity provided by Blockchain relies on the use of public key based digital signatures, hash functions, and the distributed nature of the database. Participants in a Blockchain are connected through a Peer-to-Peer (P2P) network and are independent of each other[2]. This architecture allows the sharing of resources[3], avoids single point of failure, and reduces the likelihood of data tampering because the data is not stored or managed by specific nodes[4,5,6].

However, there are many challenges[7] that need to be resolved in the case of distributed networks. These challenges include accountability, confidentiality, integrity, non-repudiation and authentication, due to the absence of any central authority. Another major issue is trust because there is no central authority that can resolve any ambiguities or disagreements that may occur. Blockchain resolves all these issues. Confidentiality and authentication are ensured using two-way encryption, i.e., by encrypting the data first by the sender's private key and then by the receiver's public key. To decrypt it, first the receiver's private key is used and then the sender's public key. Consequently, data remains confidential, integrity is achieved and because the data can be obtained using sender's public key, it acts as a digital signature that authenticates the data and eliminates the possibility of

non-repudiation. Trust is obtained by introducing a consensus algorithms that ensures that only valid data or transactions are recorded in the Blockchain. Blockchain also prevents double spending [8,9].

As a result of these attractive features in terms of security, scalability [10], blockchain technology has been used in various fields such as Industrial Internet of Things (IIoT) [11] smart health systems [12,13], smart voting [14], cybersecurity industries [15], financial services [16] and others [17,18]. However, due to the hype surrounding Blockchain technology, it is often suggested as a solution for almost any application these days [19]. However, there are many cases where the option of decentralization and the core technology of Blockchain result in unreasonable operating cost and poor performance [20].

These factors make it crucial to assess whether Blockchain technology is helpful in an emerging area or not. We propose a set of guidelines to answer the very fundamental questions such as: is Blockchain suitable for all the emerging areas? How can one assess if Blockchain is a suitable technology to use or not? What kinds of "tests" can we use to determine if Blockchain will be good to use for a specific application domain? By using the proposed guidelines, one should be able to determine if Blockchain is worth considering in the newly emerging area, the type of Blockchain to use, and various alternatives to the Blockchain.

1.1 | Research contributions of this work

This paper addresses the problem of objectively assessing the applicability of Blockchain to any specific application. While existing works have presented various fields and sectors where Blockchain may or may not be suitable, there are no proper guidelines to evaluate the effectiveness of Blockchain and to determine the most appropriate blockchain technology for a given application. Due to the lack of work done in this direction, a need to discuss the alternatives to traditional Blockchain arises. To address these issues, we present:

1. An overview of the fundamentals of Blockchain along with its advantages and disadvantages.
2. A framework to evaluate the applicability of Blockchain for a given application domain.
3. Alternatives to traditional Blockchain and when to use them.
4. Demonstration of our proposed framework using three case studies.

The remainder of this paper is organized as follows. Section II presents an overview of related surveys which also discuss when and where to use blockchain. Section III provides an overview of blockchain technology. Section IV presents various application domains where blockchain is being used. Section V presents our proposed framework to determine if blockchain is a suitable technology to use or not for a particular application. Section VI presents the alternatives to blockchain technology. Section VII presents some use-case applications that demonstrates the use of our proposed framework. Section VIII presents challenges and research directions. Finally, section IX presents our concluding remarks.

2 | LITERATURE SURVEY

Applications of blockchain have been widely explored in literature. E-commerce, logistic network [21,22,23], private data handling [24,25,26], smart communities [27,28,29,30,31,32], edge computing [33,34,35,36], machine learning [37,38,39] and deep learning [40,41,42,43,44] are some of the application domains and the related works in these areas. While cryptocurrencies are the most common and popular application of blockchain, they have also been explored for use in various industrial sectors. The increased visibility of blockchain technology has led to its uses in almost every application domain. However, the suitability of blockchain for an application depends on its specific requirements. There must be some framework to help decide on the suitability of blockchain for its deployment in a specific application domain.

In [45,46] the authors discussed a scenario where a blockchain can be used to assist a business. The authors of [47] did a brief comparison between various proposed decision models for evaluating blockchain's suitability. In [48,49,50], the authors gave some criteria to decide whether blockchain is a good option or not. The article [48] focused mainly on the use cases related to the insurance sector. The advantages and disadvantages of using blockchain in different insurance related use cases are discussed. However, the use of blockchain alternatives in some other use cases where decentralization is required, but other features of blockchain are not needed, is not discussed. The authors of [51] present some problems that can be solved with similar efficiency as blockchain at a low cost. The authors focused on helping architects, developers, investors, and project leaders evaluate the suitability of blockchain for a particular application. The solutions or the alternatives for the issues raised are not discussed in detail. Similarly,

the authors of[52] presented a detailed review of blockchain technology and they also discussed some of the criteria one could use to choose the type of blockchain for a particular application. However, they did not discuss the applications that need a DLT but cannot use a blockchain. For example, there is no facility in blockchain to maintain timestamp ordering. Thus, applications that can benefit significantly from distributed ledgers cannot use blockchain if they need to maintain the timestamp ordering of the transactions. But there are few other non-blockchain DLTs such as Hashgraph that can be used in such cases. In this paper, we discussed in detail, the blockchain alternatives that can help in addressing the disadvantages of blockchain while using its inherent features.

This paper addresses the limitations of existing literature by proposing a framework with a comprehensive set of guidelines to not only decide if blockchain is a suitable solution for an application area but also to determine the most appropriate type of blockchain and suggest alternatives of blockchain that may provide better results, according to the application's requirements.

3 | BLOCKCHAIN FUNDAMENTALS

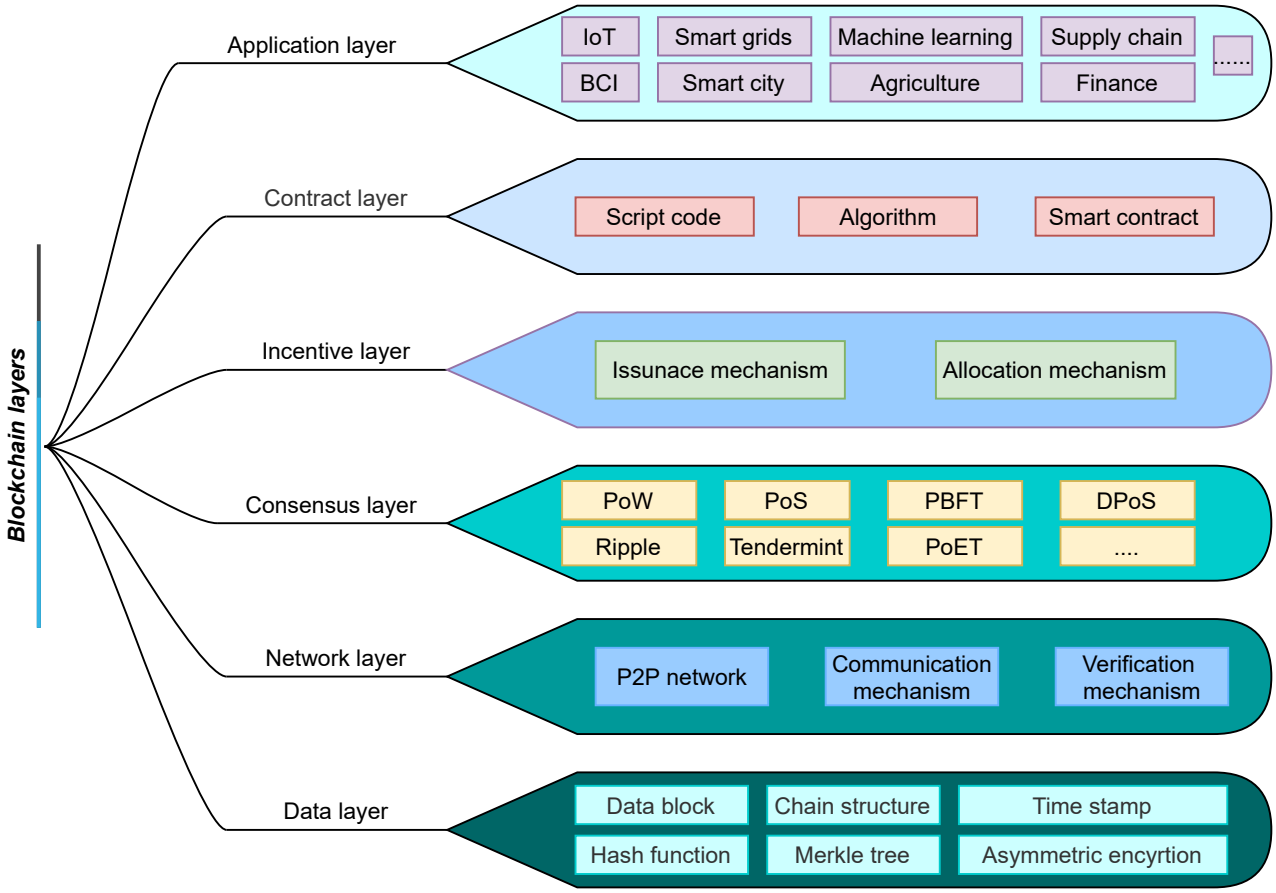

FIGURE 1 Blockchain as a multi layer framework

Figure 1 (adapted from the one proposed in[53]) shows the operation of a blockchain network can be visualized as a multi-layer framework. We discuss this multi-layered architecture below.

1. *Data layer:* The lowest layer in a blockchain architecture is the data layer. This layer contains blocks to store data. Each block consists of a body and a header. The header of the current block stores the hash of the previous block and forms a chain-like structure. The genesis block (the first block) does not contain the header as it is the first in the chain. Each block has a timestamp that is the time of its creation, a nonce which is a random number calculated by the miners to meet

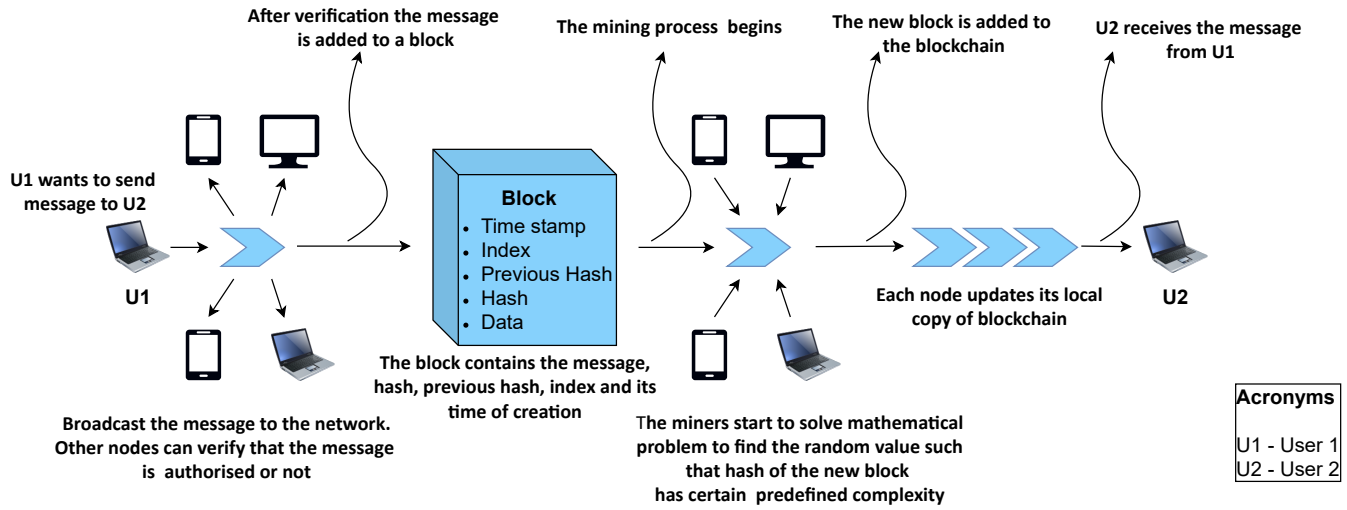

FIGURE 2 Propagation of a transaction using blockchain

the difficulty level and to get the block-hash and Merkle root which is the root of the Merkle tree (a binary tree of hashes which stores transactions).

2. *Network layer:* The main purpose of the network layer is to distribute and authenticate transactions, and facilitate inter-node communication. It is also known as propagation layer. Using a peer-to-peer (P2P) network, this layer ensures that nodes can discover and communicate with each other. Section 3.1 discusses the the flow and the life cycle of a transaction in terms of initiation, validation, and so on.

3. *Consensus layer:* This layer is central to the existence of blockchain platforms and is the most important layer for a blockchain. In a P2P network without any central authority, it is a challenging task to create consensus between every node in the network, and this is achieved in this layer. Section 3.3 discusses various types of consensus algorithms.

4. *Incentive layer:* This layer acts as a driving force in maintaining a public blockchain. It addresses the economic factor and creates economically beneficial schemes for the miners. In return for the computational power spent in the mining process, miners are rewarded with the incentives (e.g., some amount of digital currency)[54].

5. *Contract layer:* The contract layer includes different scripts, smart contracts, and algorithms to execute complex transactions securely. Smart contracts are self-executable codes with a predefined set of rules, which when met, trigger the transaction between the parties involved in the contract. These self-running codes ensure that each transaction fulfils the predefined requirements of the model. Smart contracts are fully automated, thus reducing the possibility of any fraud or theft. These contracts ensure secure transfer of digital assets involved in the transaction[55].

6. *Application layer:* This layer comprises all the applications that are used by end users. The application layer enables users to interact with the blockchain network. It includes APIs, scripts and User Interfaces (UIs). This layer provides data to the contract layer to connect users with the back-end system.

Various blockchain applications, such as cryptocurrency wallets, are found at the application level. At the contract layer or execution layer, we have the smart contracts environment that determines the nature of the transactions. The security of the network depends on the participation of nodes. The incentive layer provides incentives to motivate nodes to participate in the verification process of the blockchain. Usually, blockchain offers some amount of virtual currency as a reward to the participants. For example, bitcoin provides a few bitcoins as a reward. At the consensus layer, we have a consensus mechanism which ensures agreement among the participating nodes in a network. The network layer strategies for secure propagation of transactions. The data layer, provides a data structure to store data and perform various operations on data storage.

3.1 | Life cycle of a transaction

Transactions in blockchain are not restricted to just finance and include several other types of information, and the process of recording a transaction involves many steps [56,57]. These include instructions such as querying, sharing and storing. Once a transaction has been validated, its respective block is mined and linked to the previous block. Systems and users present in the network update their existing copy of the blockchain.

A transaction is created every time a user tries to interact with another user in the network. Depending on the blockchain system, steps in this process of a transaction may differ. Generally, it starts with the creation of the transaction and ends when it gets recorded in the blockchain (as shown in Fig 2). Hence a transaction passes through three phases:

1. *Start:* Every blockchain has its predefined data structure. Each transaction is defined, according to the data model of that blockchain, the sender, and the receiver of the digital asset. The transaction must fulfil the conditions of the smart contract or simple scripts (depending on the model).

2. *Validation:* In this step, transactions are verified by validating peers. These transactions are then inserted into a block, which is ready to be mined.

3. *Mining:* In this step, miners solve a mathematical problem, using their computational power, to find a random value such that the hash of the new block has certain predefined complexity [58,59]. This block is now added to the main blockchain.

4. *Termination:* The updated blockchain then propagates in the network to inform each node to update its own copy. Once the block is added to the blockchain, its assets are transferred accordingly.

TABLE 1 Comparison between different types of blockchain

Type of blockchain	Advantages	Disadvantages	Applications	Some Domains Using This Type
Public blockchain	Open to everyone High transparency High trust among users	Low transaction speed Low scalability High computational power	Bitcoin Ethereum Litecoin NEO	Transparency in Fundraising Voting
Private blockchain	Low transaction time Scalable	Centralized Low trust	Multichain Hyperledger fabric	Internal voting Supply chain
Consortium blockchain	High control over resources High scalability Secure	Less transparent Less anonymity	Marco Polo Energy Web Foundation IBM Food Trust	Food tracking Banking and payments
Hybrid blockchain	Closed ecosystem Immune to 51% attacks good scalability	Less transparent Complex structure	Dragonchain XinFin's Hybrid Blockchain	Real estate financial markets

3.2 | Types of Blockchain

1. *Public:* In this type of blockchain (also known as *permission-less blockchain*) anyone can join and perform transactions, i.e., anyone with an Internet connection can access a permission-less blockchain. For example, Bitcoin is one of the first public blockchains [60].

   Verification of transactions and creation of blocks are both done by the participating nodes. This implies that public blockchain becomes non-functional if it does not have the required nodes to participate in the validation process.

2. *Private:* Private blockchain (also known as permissioned blockchain) works in a restricted environment (closed network). This type of blockchain is effective for an organization that wants it for internal use-cases. In a private blockchain, only

selected participants who have permission can access the blockchain[61]. Moreover, the network is maintained by a central authority, and hence, it not decentralized in nature.

3. *Consortium:* Consortium blockchain or *federated blockchain* is an effective solution to provide an environment with both public and private blockchain features, i.e., in this type of blockchain, some attributes of the organization are made public and remaining are made private[62]. Although consortium blockchain is not open publicly, it stills manages to be decentralized in nature because it is managed by more than one organization. A validator node can initiate or receive transactions and can also perform validation of the transactions. On the other hand, member nodes can only receive or initiate transactions[63].

4. *Hybrid:* A hybrid blockchain is a combination of private and public blockchain. It combines the advantages of both private and public blockchains while limiting their disadvantages. In a hybrid blockchain, a ledger can be made accessible to everyone (publicly) by employing a public blockchain with a private blockchain that can control access to the modifications in the ledger. Ripple network is an example of a hybrid blockchain.

Each blockchain type has its advantages and disadvantages. It is vital to understand the needs of an organization or application and then choose the type of blockchain accordingly. Table 1 presents a comparison between the types of blockchain.

3.3 | Trusting the untrusted

A secure transaction can be achieved with the help of smart contracts. However, the decentralized system architectures(as in blockchain) hamper the building of trust and tend to raise questions about the probability of date modification. To maintain the integrity of the data, it has to be immutable. To achieve this goal, blockchain uses *consensus algorithms* that allow a block to be added to the blockchain only when it is agreed by all the nodes present in the network. These algorithms ensure that the data in the database (i.e. in the blockchain) cannot be altered or modified after it is stored in the blockchain [64,65].

3.3.1 | Consensus Algorithms

Initially algorithms such as: 2 phase commit (2PC)[66], atomic broadcast, State Machine Replication (SMR)[67], Byzantine Fault Tolerant (BFT)[68] were proposed to achieve a consensus in distributed databases. These algorithms have low failure-resilience. For example, in the case of 2PC, the consensus procedure gets compromised with the failure of any node. These algorithms were the precursors of consensus solutions for distributed ledger technologies. Blockchains such as Bitcoin and Ethereum achieve consensus and maintain a coherent view among participants. Such networks are failure-resilient as long as malicious nodes remain a minority. To achieve this by charging nodes who differ from the default behavior, computational cost is introduced as a *proof of Work (PoW)* that is needed to add a block in the blockchain. Bitcoin uses PoW to prevent it from a *Sybil attack*[69]. PoW has low scalability and high latency and requires a significant amount of computational power. There are several alternatives for POW to avoid complexity and wastage of computational power. We discuss some of these alternatives below.

i) *Proof of work:* In this consensus mechanism every blockchain node willing to mine or validate a block solves a complex mathematical problem that requires significant computational power[70]. To solve the problem the participants have to find a hash value of the block such that it meets a certain predefined difficulty level. The node which finds the solution first is the winner and it can create a block of transactions.

ii) *Proof-of-stake:* The PoS works are similar to PoW but the leader is chosen based on the stakes owned by the users of that network. The assumption here is, that the user with more stakes (commitment) has less probability of being a malicious node and would not attack the blockchain. This mechanism has a high chance of becoming centralized as rich committees have more voting power and may win every election. To overcome this problem and the *nothing at stake attack* variations of PoS have been proposed[71]. To work more efficiently, the algorithm can have restricted elections, i.e., *delegated proof-of-stake* (DPoS). Proof of Elapsed Time (PoET)[72] and Proof-of-Importance (PoI) are some alternatives that prevent centralization of voting[73].

iii) *BFT:* The Byzantine Fault Tolerant (BFT) algorithm guarantees consensus in a network the if at least 2/3 of the participating nodes are not malicious[74]. This algorithm is not a good option for a public blockchain because BFT can only work with

TABLE 2 A comparison between various consensus mechanisms

Reference	Consensus algorithm	Type of DLT used	Advantages	Open issues
[75,52]	Proof of Work	Permissionless	High node scalability	High computational power
[52]	Proof of Stake	Both types	High tolerance power	Low throughput
[76]	Leased Proof-of-Stake	Both types	Prevents centralization like in Proof-of-Stake	Low throughput
[77]	Delegated-Proof-of-Stake	Both types	High throughput	High Message overhead
[52,77]	Proof of Elapsed Time	Both types	Partial energy saving	Medium throughput
[75]	Byzantine Fault Tolerant	Permissioned	High energy saving	Low node scalability
[76]	Proof-of-Activity	Both types	Immune to 51% attack	High computational power
[78]	Proof-of-Capacity	Permissionless	Cheap and efficient	Less Decentralization
[79]	Proof-of-Burn	Permissionless	Greater price stability	High waste of currency
[80,81]	Tangle	Both types	High scalability	Conflicts in sparse network
[82]	Hashgraph (virtual voting)	Both types	Byzantine Fault Tolerant	Large size of signatures

a limited number of participants. The objective of this mechanism is to protect the network from system failures through collective decision making.

iv) *Proof of Elapsed Time:* This algorithm randomly chooses the next block using fair means. Every node willing to validate blocks gets a chance to create their block by waiting for a random amount of time. Each validator adds its waiting time in its block as a proof of their waiting, and broadcasts its block in the network. The validator with the least waiting time is the winner and its block gets added in the blockchain.

3.3.2 | Comparison Between Consensus Algorithms

The previous section has discussed various consensus algorithms and problems in achieving consensus in DLTs. Comparative studies on different consensus algorithms have been presented in[83],[75],[77] in terms of energy-saving, scalability, latency, throughput, and so on. Table 2 presents a summary that compares these studies.

4 | BLOCKCHAIN APPLICATION DOMAINS

With the increasing demand for distributed architectures[84], blockchain provides a possible solution for applications in various domains. In[85] the authors have discussed numerous domains (such as healthcare, smart grids and IoT.) in which blockchain has been used or has a great potential to be used[86]. Some of these domains are discussed below. For each domain, we describe the potential for using blockchain and issues that need to be overcome.

4.1 | Blockchain and Internet of Things (BIOT)

With the advancements in technologies, users are shifting toward smart devices and Internet of Things (IoT). More than 20 billion smart devices and IoT devices are currently in use[87]. The biggest strength of IoT that makes it a potentially viable option in many sector is its ability to share data between various devices and provide easy access[88,89].

The ability to share data[90] also comes with various challenges such as security, privacy, and building trust[91,92]. This becomes even more critical in domains such as healthcare, finance, defense where often there is sensitive information that needs to be protected. Blockchain provides a robust solution to address these problems as it provides a platform to safely exchange information among untrusted users [93,94,95,96]. Furthermore, the distributed nature of blockchain eliminates the risk of a single point of failure in the IoT system. We discuss some specific applications of blockchain below.

1. *IoT in Industries*

IoT has proven to be a promising technology in various industrial sectors by providing real-time remote monitoring, low-latency, smart asset tracking, and so on [34]. However, there is a high risk of attacks related to security and privacy on IoT devices. Blockchain can help mitigate these issues and provide data immutability. Many researchers have worked in this domain and have explored the challenges posed by blockchain in industrial IoT along with their possible solutions [97,98,99].

2. *IoT for Smart Grids*

   Blockchain can reduce costs and remove intermediaries in the energy sector [100,54]. This distributed platform allows trading of energy with various distributed sources [101] without the need for a centralized authority. Issues such as security and privacy are critical when it comes to a smart grid system integrated with IoT. A secure, cost-effective and reliable solution to build an infrastructure for a smart grid using blockchain has been proposed by the authors in [102].

4.2 | Blockchain and Healthcare

Major stakeholders for information exchange in the healthcare sector include patients, doctors, pathology, health-insurance company and regulation committees. Healthcare systems require an efficient solution to share information such as patient's updated profiles between all the stakeholders. Blockchain provides this solution along with ensuring patient's privacy, data immutability and restricted access to the data (for security purposes) [103]. Blockchain can be used for a variety of applications in the healthcare sector which include [104]:

1. *Secure interoperability of health records:* Health-related data is very critical and personal. Hence there should be a robust platform to exchange healthcare data between various stakeholders. The authors in [105] proposed a blockchain based scheme for secure and integrated inter-operability of health related data among stakeholders. They developed a design to validate the information in a transaction and also discussed the structure of a smart contract that ensures the fulfilment of the required conditions.

2. *Healthcare supply chains:* In the case of pharmaceutical drugs supply, many factors such as time duration, surrounding conditions (such as temperature, humidity, etc.) play a crucial role in ensuring a safe delivery. In [106], the authors have proposed a framework to use blockchain to provide a record of factors such as temperature during the transportation of pharmaceutical drugs to various stakeholders. This empowers the company to perform quality control of its products [107].

4.3 | Blockchain in business

Blockchain provides a robust platform to build a tamper-proof and secure distributed digital ledger which is supported by a consensus mechanism [85,108]. The append-only, immutable and secure nature of blockchain makes it a prominent option for a variety of businesses. Blockchain along with a smart contact, fulfils the basic requirement of any business-related use case [109]. This technology can be used for a variety of business-related use cases such as:

1. *Outsourcing in cloud-based business:* Cloud computing has become a widely accepted paradigm for outsourcing services. Cloud computing enables an organization to economically and scalable access advanced services by outsourcing them [110]. Some of the major issues in outsourcing services are data security and digital payment [111,112]. One option is to only involve a trusted third-party for outsourcing, but this becomes inefficient in the growing competition, as there can be a some untrusted third-party offering better services. The authors of [113] have proposed a blockchain-based solution to outsource any third-party, even if it is not trusted.

2. *Real estate* The real estate ecosystem deals with sales and purchase of digital or physical assets such as land, building or company shares. Various parties (e.g. owner, purchaser, tenant, broker) are involved in this process, thereby increasing the risk of record tampering or modification. Another major issue is dealing with untrusted parties because entities might not have any previous business relationships. Smart contracts can solve these issues [114] and can further eliminate the need for trusted intermediaries such as brokers and notaries [115]. In [116,117] the authors have discussed the potential use of blockchain in secure banking.

Some other domains where blockchain can be used include: agriculture [118,119], communication [120], automobile industry [121,122], and so on.

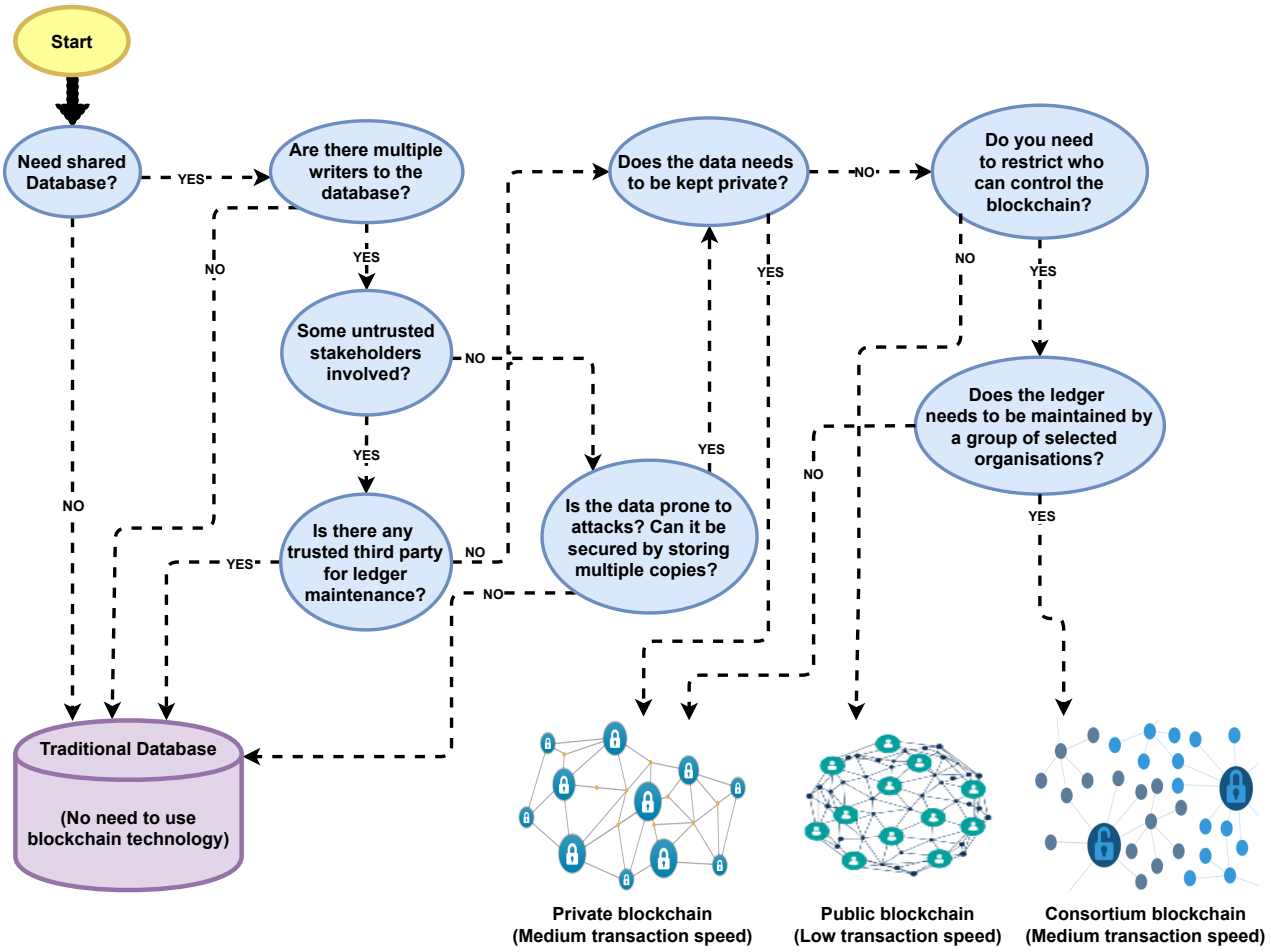

FIGURE 3 Framework for evaluating the application of blockchain technology. Black arrows represent the answer for the respective question.

Sections III and IV presented a brief overview on the fundamentals of blockchain, their application domains and consensus mechanisms. In the next section, we present a framework to evaluate the suitability of blockchain to any given application and discuss the criteria used by the proposed framework.

5 | FRAMEWORK FOR EVALUATING THE USE OF BLOCKCHAIN

The performance characteristic of blockchain under different metrics and operating conditions form the basis of the proposed framework for evaluating blockchain's applicability and suitability. We first present an overview of the advantages and disadvantages of blockchain, and then use them to develop the proposed framework.

5.1 | Advantages and disadvantages of Traditional blockchain

The main advantages and disadvantages of traditional blockchain technology include:

5.1.1 | Advantages

i) *Distributed:* The systems and the data of a blockchain are highly resilient to malicious attacks and technical failure because the data is stored in a large number of nodes present in a distributed network. Each node has its own copy of the database

and this eliminates the risk of a single point of failure. Also, even if a node goes offline, it does not affect the security and availability of the network.

ii) *Stability:* Once a block is confirmed, it is very difficult to change or modify the data stored in it. This immutability of the data makes blockchain an attractive option to store data that is sensitive to any alterations and needs to be protected against modification.

iii) *Trustless environment:* Involvement of a trusted intermediary party is often required in the traditional payment systems, such as banks and payment providers. Blockchain eliminates this need for intermediaries because the transactions, in the distributed network of nodes, are verified through a mining process. Hence, there is no need to trust a single organization which also reduces the costs of intermediaries.

5.1.2 | Disadvantages

i) *Low transaction speed:* As each transaction has to be stored on the blockchain, it takes time to gather all the transactions and accumulate them in a block. Although there may be a large number of transactions packed into a single block, and the average block processing time is about 10 minutes, the transaction speed is theoretically 100 transactions per minute. However, in practice, all those transactions get confirmed only after the block is mined and that takes around 10 minutes (on average). Hence, the transaction time on blockchain is fairly high[123].

ii) *High data requirement:* Blockchain stores a copy of every transaction that has occurred till date on that network, simultaneously, on all the computers/nodes connected to the network. This is a highly data-consuming process and the current bitcoin blockchain is about 1 TB in size and is growing daily.

iii) *High energy-consumption:* The consensus algorithm used in traditional blockchain is proof of work. The POW technique of computing hashes consumes a lot of energy because a large number of computers connected on the blockchain network simultaneously compete against each other to find an appropriate hash. It is estimated that the total energy consumed by the miners on the Bitcoin Blockchain network is equivalent to the energy requirement of a decently sized European country.

iv) *Pseudo anonymity:* Due to the decentralized nature of blockchain, transaction information are made public in the cryptocurrency. Hence, user privacy may be compromised. In[124], the authors have proposed a Quasi-Homomorphic Symmetric Encryption (QHSE) scheme to hide the transaction amounts in a blockchain based cryptocurrency. In[125], the authors combined ring signature technology with the existing blockchain system to ensure user privacy in the transparent environment of blockchain.

5.2 | Steps to assess "when" to use blockchain

In the previous section we presented an overview of blockchain, its advantages and disadvantages, and various domains where it can be used. This section addresses the main question "when to use blockchain technology?" The proposed framework to answer this question is based on assessing use-case oriented simple questions as Fig. 3 shows. The questions in this framework not only help to assess the suitability of blockchain for an application but they it also help to determine the most suitable blockchain technology

i) *Do you need a shared database?:* We assume that there is a need of a ledger database, i.e., some data related to transactions needs to be stored. Data represents the present state of the ledger, which gets updated and must be shared. However, if data does not need to be shared, a complex blockchain-based architecture is not needed. Therefore, blockchain is not required if the answer is "no" and traditional databases are preferred.

ii) *Are there multiple writers to the database?:* Opting for blockchain only makes sense when multiple copies of the data has to be stored (by multiple users) and shared among them[52]. In a blockchain, multiple users have permission to maintain the ledger and establish consensus among the users. In contrast to traditional server-client architectures with restricted writing rights, blockchain provides an alternate option of a decentralized peer to peer network where multiple users can write to the distributed ledger.

iii) *Are there untrusted stakeholders involved?:* Blockchain provides a robust solution to conduct transactions even if the parties or stakeholders involved are not trusted. If only trusted parties are involved and data is not very sensitive (not prone to attacks or modification) then using a traditional database is preferable. However, in scenarios where the possibility of choosing a third party to establish consensus in an untrusted environment is available, using a centralized architecture is preferred.

iv) *Does the data need to be kept private?:* If no external entity is involved to provide trust management services or if the data is sensitive (even if all stakeholders are trusted) then opting for blockchain technology is effective and should be considered. If data has to be kept private, maintaining a private blockchain is a good option.

v) *Do we need any restriction on who can control the blockchain?:* If the answer to the previous question on the need for data to be kept private is a "no", and if there is no restriction to control the blockchain (i.e., the system is maintained by a public community and all the transactions are transparent and visible to everyone) then having a public blockchain is preferable.

vi) *Does the ledger need to be maintained by a group of selected organizations?:* If maintenance of the ledger cannot be done publicly, and a group of some selected organizations needs to be chosen to entrust system maintenance, the use of a consortium blockchain is preferable. Consortium blockchain has the advantages of a public blockchain (transparent, available for all) as well as those of a private blockchain (controlled by more than one organization, which makes it decentralized). A private blockchain is preferred if there must be only one organization that can control and maintain the ledger [126].

6 | ALTERNATIVES TO TRADITIONAL BLOCKCHAIN TECHNOLOGY

The previous section, described the drawbacks of using blockchain technology. Apart from blockchain technology, there are numerous other options that one may consider (if blockchain is not a suitable solution after assessing the above criteria). The following section presents similar technologies and alternatives (figure 4 presents an overview).

6.1 | Hashgraph

Hashgraph is a distributed ledger technology that uses an algorithm for duplication of state machines in order to ensure Byzantine Fault Tolerant (BFT) [127]. This is sometimes also referred to as an atomic broadcast. The main protocol that runs this DLT is a gossip protocol. In this protocol, every node needs to share all its information and transactions with any other randomly selected node. The gossip protocol supports nesting which refers to the fact a gossip can also have another gossip built in it. All participants (nodes) in the network receive an identical chronologically arranged list of transactions referred to as “total order”. The implementation and feasibility part of Hashgraph is still questionable as this is not an open-source protocol.

1. *Data structure:* The data structure used in Hashgraph is a Directed Acyclic Graph with each transaction itself acting as a block in-itself. It has information such as signature, timestamp, transaction hash and hash of the parent transaction.
2. *Consensus algorithm:* Hashgraph uses an innovative virtual voting [128] consensus method which sends out transactions to the network as an Atomic Blast Broadcast.
3. *Advantages over Traditional Blockchain:*

   i) Hashgraph is a proprietary DLT and hence tampering with it is difficult. This is a significant benefit in terms of human exposed vulnerability.
   ii) Due to its gossip protocol, the net transactional data that nodes have to store is significantly lower.
   iii) As this DLT does not involve block formation and waiting for each block to get transactions confirmed, the speed of transactions is fairly high. Theoretically, it is possible to even reach the speed of 1,000,000 TPS (transactions per second) on the Hashgraph protocol

   As a result of these advantages, Hashgraph offers a variety of applications in today’s technology-driven world. Having a fast consensus algorithm enables the Hashgraph cryptocurrency to have low network fees, making small microtransactions economical, particularly in IoT applications. Hashgraph enables users to store decentralized data or pointers to files on the network in a secure and transparent manner. It also enables users to deploy smart contracts. Solidity language was developed for executing smart contracts on the Ethereum network although various libraries of Solidity code have been developed after, and can be run on the Hashgraph platform [129].

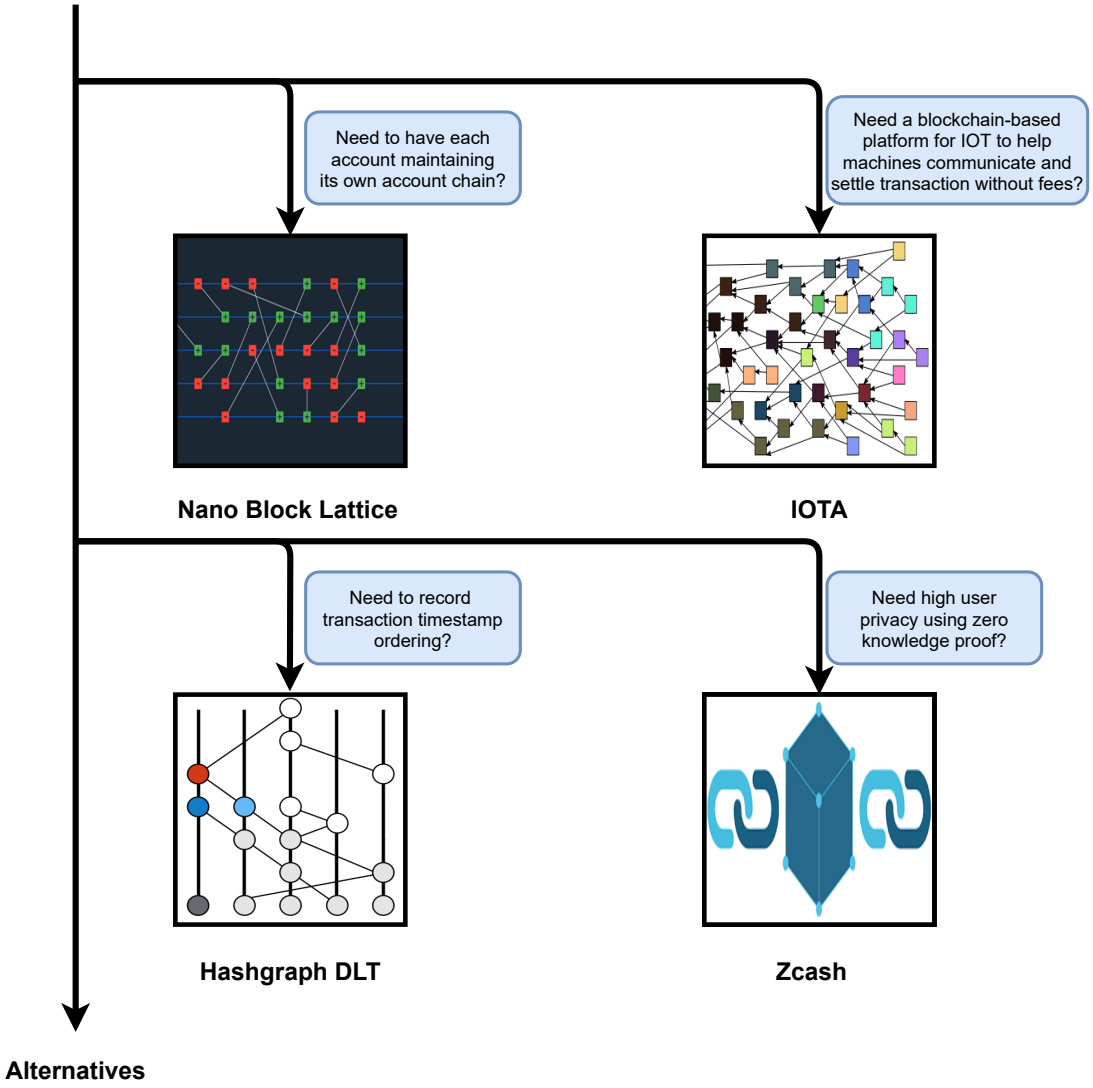

FIGURE 4 Blockchain alternatives and when to select them.

6.2 | IOTA

IOTA uses a distributed ledger technology called the Tangle. Tangle is similar to the traditional blockchain in the sense that it stores the history of transactions in an immutable data structure. Unlike the Bitcoin blockchain, the Tangle protocol involves attaching each transaction to two previous transactions through their hashes. This drastically reduces the amount of data required for storing transactions.

1. *Data structure:* The data structure of IOTA is a Directed Acyclic Graph (DAG). In this data structure, each transaction can be referred either directly or indirectly. Trunk transaction field of any transaction stores transaction hash of either an existing transaction in the Tangle or of the transaction with the next index in the bundle. The direct references of a transaction are called its Parents, and indirect ones as grandparents, similar to a family tree. Every new transaction on this network starts as a tip transaction of the DAG. These are then chosen by nodes after validating them.

2. *Consensus algorithm:* The latest consensus algorithm for IOTA is fast probabilistic consensus with weighted votes which is an upgrade from the earlier Tangle protocol. This is a Byzantine-tolerant consensus algorithm where the voting power of a node is proportional to its reputation. The reputation of the node is modelled using the Zipf law which shows that

the performance of the algorithm increases with the Zipf exponent. Zipf law is used because it best describes Mana distribution.

3. *Advantages over traditional Blockchain:*

   i) Due to its highly scalable infrastructure, the IOTA DLT can be used for IoT device's transactional data.

   ii) IOTA, similar to Hashgraph, has a Directed Acyclic Graph data structure that enables it to achieve fast transaction times. Hence, it is nearly 100 times faster than traditional blockchain.

   iii) As this DLT does not involve block formation and waiting for each block to get transactions confirmed, the speed of transactions is fairly high. Theoretically, it is possible to even reach the speed of 1,000,000 Transactions Per Second (TPS) on the Hashgraph protocol.

   Having advantages such as high transaction rate along with a resilient architecture[130], IOTA provides a large application base. For example, the authors[131] used the IOTA cryptocurrency to propose a privacy-preserving tolling architecture that supports decentralized feeless transfers for providing communication with roadside infrastructures. The proposed approach incorporates several technologies that work together to provide convenience and value to drivers and road operators.

6.3 | Nano Coin

Nano coin (also known as RaiBlocks) is one of the first coins to use no-fee transfers. Instead of using the traditional blockchain structure, Nano coin use the Block Lattice structure. This enables it to achieve high transaction speed at very low to no fees. The consensus method used by Nano coin involves Proof of Stake (PoS) where any offender in the network is punished by foreclosing his/her stake that was put into the network while joining. There are nodes in the network whose function is to solve disputes when a collision transaction arises. These nodes lose their stake of coins if found guilty of approving a false transaction.

1. *Data structure:* The data structure of Nano coin is not like that of a traditional blockchain. Nano coin uses the Block Lattice structure wherein each address on the network has its own blockchain (address chain).

2. *Consensus algorithm:* Nano coin uses a combination of both Proof of Stake and Proof of Work as its consensus mechanism. This hybrid mechanism is also called *Delegated Proof of Stake*.

3. *Advantages over traditional Blockchain:* Nano coin has one of the highest transaction per second speed and hence it is one of the best choices for micropayment platforms. Nano coin was one of the first to adopt directed cyclic graphs and paved the way for subsequent technologies such as Hashgraph IOTA to come up with a more robust and fast DLT.

6.4 | Zcash

Zcash is a privacy-centric digital currency that uses a zero-knowledge proof based technique for encryption. Zcash uses two types of addresses that are either private or transparent. The transactions among the Z addresses, i.e., private or shielded addresses, need not be disclosed publicly. On the other hand, the T addresses, i.e., the transparent addresses, work in a similar manner to a bitcoin address where the transactions are visible to the entire world[132]. Some of the salient features of Zcash are:

i) *Minimum transaction fees:* The transaction fee on the Zcash network is one of the lowest among all cryptocurrencies (0.0001 ZEC).

ii) *Privacy:* The core principle of Zcash is to ensure consumer privacy. This is achieved by using two types of addresses (shielded and transparent). Shielded addresses are not visible publicly. Addresses and transaction details (e.g. transaction amount) are not revealed in a transaction between shielded addresses. On the other hand, transactions between transparent addresses are publicly viewable on the network.

iii) *Time-based and multiple signature-based transactions:* At times when a transaction is not mined for a long time, Zcash provides the facility to refund the transaction. Zcash also has the feature of multiple signatures which enables the production of large funds through the approval of multiple parties.

Multiple address types (private and transparent) enable different types of transactions in the network:

i) *Shielding:* Transaction from transparent address to a private address

ii) *Public:* Transaction from transparent adding to a transparent address.

iii) *De-shielding:* Transaction from private adding to a transparent address.

iv) *Private:* Transaction from private adding to a private address.

1. *Data structure:* The data structure of Zcash is the same as that of a traditional blockchain.
2. *Consensus algorithm:* Zcash uses Proof of Work as its consensus mechanism.
3. *Advantages over traditional Blockchain:* As we mentioned earlier, a special feature of Zcash is its privacy protection for users. With the help of zero-knowledge proof encryption, the privacy of the users is kept intact without making any compromises on the network security.

TABLE 3 A comparison between alternative technologies to blockchain

	Hashgraph	**IOTA**	**Nano Coin**	**Zcash**
Consensus mechanism	Atomic blast Broadcast	FPC with weighted votes	Delegated proof of stake	Proof of Work
Data Structure	Directed Cyclic Graph	Directed Cyclic Graph	Block lattice structure	Traditional blockchain
Scalability	Highly scalable	Highly scalable	Moderately scalable	Least scalable
Privacy	Pseudo anonymous	Pseudo anonymous	Pseudo Anonymous	Protects privacy
Transaction Rate	10 Transactions/sec	11 Transactions/Sec	105 Transactions/Sec	3 Transactions/Sec
Token needed	Yes	Yes	Yes	Yes

The four alternative technologies described above have unique advantages and disadvantages. It is vital to understand the application's or scenario's need and choose the technology accordingly. Table 3 presents a brief comparison of these technologies. For example, Hashgraph and IOTA are highly scalable. On the other hand, Zcash is not so scalable but it provides better privacy options. These technologies may fulfill specific needs of a user (as shown in Figure 4) which a simple blockchain is unable to do so. i) *Nano block lattice* gives the ability to an account to maintain its own account chain; ii) *IOTA* enables a blockchain-based IoT platform to help machines communicate and perform transactions without any fee; iii) *Zcash* provides high user privacy and uses zero knowledge proof mechanism; iv) *Hashgraph* enables to store transaction timestamp ordering in a distributed ledger, which is vital for a network where the order of requests has a high priority [133].

7 | USE-CASE APPLICATION

Section V presented the proposed framework for evaluating the applicability of blockchain. In this section, we demonstrate the application of the framework to three test cases namely supply chain, multi-drone network and financial services. Table 4 presents a summary of the results.

TABLE 4 Analysis of use cases based on the proposed criteria. "NA" means the particular question does not need to be answered.

	Supply chain	Multi drone network	Financial services
Do we need a shared database?	Yes	Yes	Yes
Are there multiple writers to the database?	Yes	Yes	Yes
Untrusted stakeholders involved?	Yes	Yes	Yes
Is there any trusted third party for ledger maintenance?	No	No	Yes
Does the data need to be kept private?	No	No	NA
Is the data prone to attacks? Can it be secured by storing multiple copies?	NA	NA	NA
Do we need to restrict who can control the blockchain?	Yes	No	NA
Does the ledger needs to be maintained by a group of selected organizations?	No	NA	NA
Do we need to have each node maintaining its own account chain?	No	No	No
Do we need a blockchain-based platform for IoT to help machines communicate and settle transaction without fees?	No	No	No
Do we need to record transaction timestamp ordering?	No	Yes	No
Do we need high user privacy using zero knowledge proof?	No	No	No

7.1 | Supply chain

Supply chain management is the management of the transitions of goods and services and includes all processes involved in the transformation of raw materials into final products. It defines the life cycle of a product, from the manufacturer to the end-consumer. Generally, stakeholders at different levels do not have access to the products' information as a whole. This results in inefficiency during the processing and transfer of products between the different stakeholders in a supply-chain [134]. Blockchain can significantly improve the transparency in a supply chain [135] by providing the products' information to all the actors in the process in its entirety [136] [137]. Moreover, it enables end-consumers to monitor and trace the products' transition with the help of IoT devices. The food system, for example, is very complex, and includes producers, processors, distributors and consumers. The sharing of information in this complex network is challenging. However, blockchain with the help of IoT devices, can give the consumers the ability to not only track where the product came from but how was it produced (e.g., if it was produced safely, if it grows sustainably, and so on). Since 2016, AgriDigital has pioneered, the use of blockchain across agricultural supply chains.AgriDigital and CBH Group, conducted a pilot to test the application of blockchain in the Australian grain industry at CBH's wholly owned subsidiary, Blue Lake Milling, an oats processor in Bordertown, South Australia. To formally evaluate the applicability of blockchain in such environments using the proposed framework, we can consider the use case of AgriDigital and CBH Group [138].

- *Do we need a shared database?:* Yes, the information needs to be registered into a ledger and communicated to all the stakeholders involved in the product's life-cycle.
- *Are there multiple writers to the database?:* Yes, supply chain management is characterized by many stakeholders such as producers, processors, distributors, retailers and consumers. All these actors interact with the blockchain.
- *Are there untrusted stakeholders involved?:* Yes, actors at different stages can be unknown and untrusted for others in the supply chain.
- *Is there any trusted third party for ledger maintenance?:* No, there is no specific third party such as a bank or notary for ledger maintenance.
- *Does the data needs to be kept private?:* No, the main objective of AgriDigital is to provide data to everyone concerned and to improve transparency in the supply chain.
- *Do we need to restrict who can control the blockchain?:* Yes, the supply chain has some restrictions on who can access the blockchain. The stakeholders involved are given permission to interact with the blockchain.
- *Does the ledger needs to be maintained by a group of selected organizations?:* No, there is no need for a specific organization to maintain the ledger.

Hence, after assessing the *when and which* part of our framework, we get private blockchain as a solution. It is worth noting that AgriDigital and the CBH Group operate on a private Quorum network. The Quorum network use the Raft consensus mechanism, which allows the AgriDigital network to have four transactions per second [138].

7.2 | Multi drone network

Recent technological advances in drone technology or Unmanned Aerial Vehicles (UAVs) in various fields such as networking,defense, manufacturing, have increased their usage in private and commercial sectors [139]. With UAV technology becoming omnipresent [140], various issues in using UAVs need to be addressed such as inter UAV communication, data storage, management in multi drone networks [141], constrained flight time, and so on. This section discusses the solution to resolve some of the issues stated above by considering a use case and applying our framework to decide if blockchain can be used for this application domain.

Multi-drone networks have a wide range of applications such as delivering goods and medical supplies, and surveillance [142]. However,one of the main constraints that hampers the applications of UAVs is their limited energy supplies (batteries are kept small to reduce the overall weight of a drone). Frequent recharging or battery replacement is required because of constrained flight time. A distributed P2P network of drones and charging stations can solve this issue and can significantly increase drones' flight time, thereby enabling the use of drones for multiple applications [133]. We now apply the proposed framework to evaluate the applicability of blockchain in multi-drone applications [143].

- *Do we need a shared database?:* Yes, communication between UAVs and charging stations is needed and information related to transactions needs to be shared and registered into a ledger and communicated to all other nodes (UAVs and charging stations) present in the network.
- *Are there multiple writers to the database?:* Yes, various drones and can enter into the network and can request charging stations to provide charging services. Each UAV should be able to interact with the ledger.
- *Are untrusted stakeholders involved?:* Yes, due to no restrictions for drones to enter into the network, unknown/untrusted UAVs may enter as well.
- *Is there any trusted third party for ledger maintenance?:* No, there is no need for any specific third party such as banks or notaries to maintain the ledger.
- *Does the data needs to be kept private?:* No, a charging station can have requests from many (if not all) drones in the network and similarly a drone needs information regarding every station present in the network.

- *Do we need to restrict who can control the blockchain?:* No, the system is free and without any restrictions. Any node present in the network can interact with the ledger.

After applying the above criteria, a public blockchain could be the appropriate technology. However, in this multi-drone system, drones should be able to enter and leave the network at a high frequency. Hence, an accurate *time-stamp ordering* is required to avoid any conflicts. From figure 4 , we note that the Hashgraph DLT is a promising solution to meet the requirement of this system. Also, Hashgraph has higher transaction throughput as compared to *hashgraph*[144]. In[133] the authors have proposed a similar Hashgraph based DLT for the specified multi-drone network.

7.3 | Financial services

Blockchain is emerging as a powerful and secure option for recording data and transactions in the financial sector. Many cryptocurrencies such as Bitcoin, Ether and Ripple. use blockchain technology and support millions of users. For example, Bitcoin had between 2.9 to 5.8 million unique users (as per[145]) in 2017. However, it still lacks scalability because it can process only a few transactions per second (Bitcoin can process 3-4 transactions per second). In contrast, other payment gateways such as the Visa Network can process over 17,000 transactions per second[146].We now apply the proposed to framework on the Visa payment processing, application.

- *Do we need a shared database?:* Yes, users need to access the database to view their transaction histories.
- *Are there multiple writers to the database?:* Yes, thousands of users make transaction every second and each transaction has to be stored in the database.
- *Are untrusted stakeholders involved?:* Yes, the company has users from all over the world, and this increases the risk of having untrusted users.
- *Is there any trusted third party for ledger maintenance?:* Yes, Visa Inc. verifies each transaction and maintains the ledger.

Hence, after assessing the above criteria, it can be concluded that having a centralized architecture is beneficial. Visa Inc. also uses a centralized architecture[147] that provides customized processing across the world.

8 | CHALLENGES AND FUTURE RESEARCH OPPORTUNITIES

Numerous blockchain-based decentralized applications are being developed due to the availability of a wide range of different blockchain technology options and their advantages available. In particular, many startups have been founded based on blockchain-related technologies since Bitcoin came into existence. However, there are still many challenges that still need to be addressed for this technology:

1. *Quantum attacks:* Quantum computing presents a major threat[148] to blockchain due to their capability in solving certain complex problems. Quantum computers can easily break existing encryption techniques[149] and may provide enough resources to perform 51% attacks in the future (Fig 5 shows various types of attacks possible of blockchain) . Various studies such as[150,151,152,153,154] have discussed such security issues.
2. *Scalability:* Many efficient consensus mechanisms are being developed to reduce the energy consumption and the time taken to process a transaction. However, blockchain still faces scalability issues when it comes to the number of transactions it can process per unit time[155].
3. *Protecting blockchain from intelligent attacks:* With the increasing possibility of more advanced types of attacks such as Machine Learning and game-theory based attacks on blockchain networks [156,157], it has become a necessity to secure blockchain against such attacks.
4. *Reducing computational power usage:* Blockchain, in general, requires high computational power which is a drain on resources. This hinders the development of the technology for many applications such as drone / UAV networks[133] where computational power is scarce.

FIGURE 5 Different types of attacks on blockchain

9 | CONCLUSION

To reap the full potential of any new technology, it has to be analyzed from various perspectives. Blockchain technology has a great potential to transform industries by providing security, transparency, anonymity and immutability. Despite being a relatively new technology, blockchain has been adopted in various fields. In this paper, we have not only provided the background behind blockchain technology, but also a framework to evaluate the applicability of blockchain technology and determined possible alternatives, if needed. With the rapid advances in technologies, the drawbacks of blockchain have been addressed to some extent. However, there is still scope for future developments and this work has identified some of the areas such as improving security against quantum attacks, reducing computational power usage and more, where research opportunities exist.

ACKNOWLEDGMENT

We thank the anonymous reviewers for their valuable comments which helped us improve presentation and content of this paper.

References

1. Kaur A, Nayyar A, Singh P. Blockchain: A path to the future. *Cryptocurrencies and Blockchain Technology Applications* 2020: 25–42.

2. Schollmeier R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. *IEEE: Proceedings First International Conference on Peer-to-Peer Computing* 2001: 101–102.

3. Hassija V, Chamola V, Garg S, Dara NGK, Kaddoum G, Jayakody DNK. A blockchain-based framework for lightweight data sharing and energy trading in V2G network. *IEEE Transactions on Vehicular Technology* 2020.

4. Goyal S. *Centralized vs decentralized vs distributed*. 2015. Available at https://medium.com/@bbc4468/centralized-vs-decentralizedvs-distributed-41d92d463868.

5. Ren Y, Zhu F, Zhu K, Sharma PK, Wang J. Blockchain-based trust establishment mechanism in the internet of multimedia things. *Multimedia Tools and Applications* 2020: 1–24.

6. Hosen AS, Singh S, Sharma PK, et al. Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network. *IEEE Access* 2020; 8: 117266–117277.

7. Jain N, Chugh K. Security Concerns of Blockchain. *Blockchain for Business: How It Works and Creates Value* 2021: 201–230.

8. Zyskind G, Nathan O, others . Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*: 180–184.

9. Giungato P, Rana R, Tarabella A, Tricase C. Current trends in sustainability of bitcoins and related blockchain technology. *Sustainability* 2017; 9(12): 2214.

10. Jogalekar P, Woodside M. Evaluating the scalability of distributed systems. *IEEE Transactions on parallel and distributed systems* 2000; 11(6): 589–603.

11. Cao J, Wang X, Huang M, Yi B, He Q. A security-driven network architecture for routing in industrial Internet of Things. *Transactions on Emerging Telecommunications Technologies*: e4216.

12. Alsamhi SH, Lee B, Guizani M, Kumar N, Qiao Y, Liu X. Blockchain for decentralized multi-drone to combat COVID-19 and future pandemics: Framework and proposed solutions. *Transactions on Emerging Telecommunications Technologies* 2021: e4255.

13. Fernández-Caramés TM, Froiz-Míguez I, Blanco-Novoa O, Fraga-Lamas P. Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care. *Sensors* 2019; 19(15): 3319.

14. Gao S, Zheng D, Guo R, Jing C, Hu C. An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function. *IEEE Access* 2019; 7: 115304–115316.

15. Fernández-Caramés TM, Fraga-Lamas P. A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access* 2019; 7: 45201–45218.

16. Hassija V, Bansal G, Chamola V, Kumar N, Guizani M. Secure Lending: Blockchain and Prospect Theory-Based Decentralized Credit Scoring Model. *IEEE Transactions on Network Science and Engineering* 2020.

17. Malomo O, Rawat D, Garuba M. Security through block vault in a blockchain enabled federated cloud framework. *Applied Network Science* 2020; 5(1): 1–18.

18. Sharma PK, Park JH, Cho K. Blockchain and Federated Learning-based Distributed Computing Defence Framework for Sustainable Society. *Sustainable Cities and Society* 2020: 102220.

19. Malik AA, Tosh DK, Ghosh U. Non-intrusive deployment of blockchain in establishing cyber-infrastructure for smart city. *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*: 1–6.

20. Singh J, Venkatesan S. Blockchain mechanism with Byzantine fault tolerance consensus for Internet of Drones services. *Transactions on Emerging Telecommunications Technologies* 2021: e4235.

21. Fanning K, Centers DP. Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance* 2016; 27(5): 53–57.

22. Maurer B. Re-risking in realtime. On possible futures for finance after the blockchain. *Behemoth-A Journal on Civilisation* 2016; 9(2): 82–96.

23. Fu Y, Zhu J. Big production enterprise supply chain endogenous risk management based on blockchain. *IEEE Access* 2019; 7: 15310–15319.

24. Truong NB, Sun K, Lee GM, Guo Y. GDPR-compliant personal data management: A blockchain-based solution. *arXiv preprint arXiv:1904.03038* 2019.

25. Guo H, Li W, Nejad M, Shen CC. Access control for electronic health records with hybrid blockchain-edge architecture. *2019 IEEE International Conference on Blockchain (Blockchain)* 2019: 44–51.

26. Mertz L. (Block) chain reaction: a blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution. *IEEE pulse* 2018; 9(3): 4–7.

27. Guan Z, Si G, Zhang X, et al. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. *IEEE Communications Magazine* 2018; 56(7): 82–88.

28. Hassija V, Bansal G, Chamola V, Saxena V, Sikdar B. Blockcom: A blockchain based commerce model for smart communities using auction mechanism. *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*: 1–6.

29. Su Z, Wang Y, Xu Q, Fei M, Tian YC, Zhang N. A secure charging scheme for electric vehicles with smart communities in energy blockchain. *IEEE Internet of Things Journal* 2018; 6(3): 4601–4613.

30. Kianmajd P, Rowe J, Levitt K. Privacy-preserving coordination for smart communities. *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*: 1045–1046.

31. Alcarria R, Bordel B, Robles T, Martín D, Manso-Callejo MÁ. A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities. *Sensors* 2018; 18(10): 3561.

32. Aggarwal S, Chaudhary R, Aujla GS, Kumar N, Choo KKR, Zomaya AY. Blockchain for smart communities: Applications, challenges and opportunities. *Journal of Network and Computer Applications* 2019; 144: 13–48.

33. Stanciu A. Blockchain based distributed control system for edge computing. *IEEE: 2017 21st International Conference on Control Systems and Computer Science (CSCS)*: 667–671.

34. Liu H, Zhang Y, Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Network* 2018; 32(3): 78–83.

35. Kang J, Yu R, Huang X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal* 2018; 6(3): 4660–4670.

36. El Ioini N, Pahl C, Helmer S. A decision framework for blockchain platforms for IoT and edge computing. In: SCITEPRESS. 2018.

37. Kurtulmus AB, Daniel K. Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain. *arXiv preprint arXiv:1802.10185* 2018.

38. Kuo TT, Ohno-Machado L. Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. *arXiv preprint arXiv:1802.01746* 2018.

39. Swan M. Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]. *IEEE Technology and Society Magazine* 2015; 34(4): 41–52.

40. Weng J, Weng J, Zhang J, Li M, Zhang Y, Luo W. Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Transactions on Dependable and Secure Computing* 2019.

41. Dai Y, Xu D, Maharjan S, Chen Z, He Q, Zhang Y. Blockchain and deep reinforcement learning empowered intelligent 5G beyond. *IEEE Network* 2019; 33(3): 10–17.

42. Luong NC, Xiong Z, Wang P, Niyato D. Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach. *2018 IEEE International Conference on Communications (ICC)*: 1–6.

43. Juneja A, Marefat M. Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. *2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI)*: 393–397.

44. Qiu C, Yu FR, Yao H, Jiang C, Xu F, Zhao C. Blockchain-based software-defined industrial Internet of Things: A dueling deep Q-learning approach. *IEEE Internet of Things Journal* 2018; 6(3): 4627–4639.

45. Wüst K, Gervais A. Do you need a blockchain?. *IEEE: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*: 45–54.

46. Koens T, Poll E. What blockchain alternative do you need?. *Springer: Data Privacy Management, Cryptocurrencies and Blockchain Technology* 2018: 113–129.

47. Meunier S. *When do you need blockchain? Decision models.* Available at https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1.

48. Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaria V. To blockchain or not to blockchain: That is the question. *IT Professional* 2018; 20(2): 62–74.

49. Peck ME. Blockchain world-Do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectrum* 2017; 54(10): 38–60.

50. Menon J. *10 Questions To Ask Before You Use Blockchain*. 2020. Available at https://rb.gy/qkusr2.

51. Scriber BA. A Framework for Determining Blockchain Applicability. *IEEE Software* 2018; 35(4): 70-77. doi: 10.1109/MS.2018.2801552

52. Belotti M, Božić N, Pujolle G, Secci S. A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials* 2019; 21(4): 3796–3838.

53. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering* 2018; 30(7): 1366–1385.

54. Miglani A, Kumar N, Chamola V, Zeadally S. Blockchain for Internet of Energy management: Review, solutions, and challenges. *Computer Communications* 2020; 151: 395–418.

55. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *2016 IEEE symposium on security and privacy (SP)*: 839–858.

56. Singh P, Nayyar A, Kaur A, Ghosh U. Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities. *Future Internet* 2020; 12(4): 61.

57. Singh PK, Singh R, Nandi SK, Ghafoor KZ, Rawat DB, Nandi S. Blockchain-based adaptive trust management in internet of vehicles using smart contract. *IEEE Transactions on Intelligent Transportation Systems* 2020.

58. Sharma PK, Kumar N, Park JH. Blockchain Technology Toward Green IoT: Opportunities and Challenges. *IEEE Network* 2020.

59. Doku R, Rawat DB. IFLBC: On the Edge Intelligence Using Federated Learning Blockchain Network. *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*: 221–226.

60. Ren Y, Zhu F, Sharma PK, et al. Data query mechanism based on hash computing power of blockchain in Internet of Things. *Sensors* 2020; 20(1): 207.

61. Ra GJ, Roh CH, Lee IY. A Key Recovery System Based on Password-Protected Secret Sharing in a Permissioned Blockchain. *CMC-COMPUTERS MATERIALS & CONTINUA* 2020; 65(1): 153–170.

62. Lin X, Li J, Wu J, Liang H, Yang W. Making Knowledge Tradable in Edge-AI Enabled IoT: A Consortium Blockchain-Based Efficient and Incentive Approach. *IEEE Transactions on Industrial Informatics* 2019; 15(12): 6367-6378.

63. Doku R, Rawat DB, Liu C. On the Blockchain-Based Decentralized Data Sharing for Event Based Encryption to Combat Adversarial Attacks. *IEEE Transactions on Network Science and Engineering* 2020.

64. Kim TH, Goyat R, Rai MK, et al. A Novel Trust Evaluation Process for Secure Localization Using a Decentralized Blockchain in Wireless Sensor Networks. *IEEE Access* 2019; 7: 184133–184144.

65. Hassija V, Chamola V, Krishna DNG, Kumar N, Guizani M. A Blockchain and Edge Computing-based Secure Framework for Government Tender Allocation. *IEEE Internet of Things Journal* 2020.

66. Gray JN. Notes on data base operating systems. In: Springer. 1978 (pp. 393–481).

67. Schneider FB. Implementing fault-tolerant services using the state machine approach: A tutorial. *ACM Computing Surveys (CSUR)* 1990; 22(4): 299–319.

68. Lamport L, Shostak R, Pease M. The Byzantine generals problem. In: 2019 (pp. 203–226).

69. Aspnes J, Jackson C, Krishnamurthy A. Exposing computationally-challenged Byzantine impostors. tech. rep., Technical Report YALEU/DCS/TR-1332, Yale University Department of Computer . . . ; 2005.

70. Li J, Zhou Z, Wu J, et al. Decentralized On-Demand Energy Supply for Blockchain in Internet of Things: A Microgrids Approach. *IEEE Transactions on Computational Social Systems* 2019; 6(6): 1395-1406.

71. Li W, Andreina S, Bohli JM, Karame G. Securing proof-of-stake blockchain protocols. In: Springer. 2017 (pp. 297–315).

72. Olson K, Bowman M, Mitchell J, Amundson S, Middleton D, Montgomery C. Sawtooth: An Introduction. *The Linux Foundation, Jan* 2018.

73. Hassija V, Saxena V, Chamola V. A mobile data offloading framework based on a combination of blockchain and virtual voting. *Software: Practice and Experience* 2020.

74. Castro M, Liskov B, others . Practical Byzantine fault tolerance. *OSDI* 1999; 99(1999): 173–186.

75. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE international congress on big data (BigData congress)*: 557–564.

76. ANWAR H. *Consensus Algorithms: The Root Of The Blockchain Technology*. Available at https://101blockchains.com/consensus-algorithms-blockchain/amp/#6.

77. Bach L, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms. *IEEE: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*: 1545–1550.

78. Grigorchuk K. *Overview of 9 blockchain consensus algorithms*. Available at https://digiforest.io/blog/blockchain-consensus-algorithms.

79. kenton W. *Proof of Burn (Cryptocurrency)*. 2020. Available at https://rb.gy/3vqyqv.

80. Shafeeq S, Zeadally S, Alam M, Khan A. Curbing Address Reuse in the IOTA Distributed Ledger: A Cuckoo-Filter-Based Approach. *IEEE Transactions on Engineering Management* 2020; 67(4): 1244-1255. doi: 10.1109/TEM.2019.2922710

81. Bramas Q. The Stability and the Security of the Tangle. 2018.

82. Wall E. *Hedera Hashgraph — Time for some FUD.* 2019. Available at https://medium.com/@ercwl/hedera-hashgraph-time-for-some-fud-9e6653c11525.

83. Cachin C, Vukolić M. Blockchain consensus protocols in the wild. *arXiv preprint arXiv:1707.01873* 2017.

84. Weber I, Xu X, Riveret R, Governatori G, Ponomarev A, Mendling J. Untrusted business process monitoring and execution using blockchain. *Springer: International Conference on Business Process Management* 2016: 329–347.

85. Syed TA, Alzahrani A, Jan S, Siddiqui MS, Nadeem A, Alghamdi T. A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. *IEEE Access* 2019; 7: 176838–176869.

86. Jindal A, Aujla GSS, Kumar N, Villari M. GUARDIAN: Blockchain-based secure demand response management in smart grid system. *IEEE Transactions on Services Computing* 2019.

87. Statista I. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). 2018.

88. Alladi T, Chamola V, Parizi RM, Choo KKR. Blockchain applications for industry 4.0 and industrial IoT: A review. *IEEE Access* 2019; 7: 176935–176951.

89. Praveen G, Chamola V, Hassija V, Kumar N. Blockchain for 5G: A Prelude to Future Telecommunication. *IEEE Network* 2020.

90. Narayanaswamy J, Sampangi RV, Sampalli S. SCARS: Simplified cryptographic algorithm for RFID systems. : 32–37.

91. Yang Q, Lu R, Rong C, Challal Y, Laurent M, Wang S. Guest editorial the convergence of blockchain and iot: Opportunities, challenges and solutions. *IEEE Internet of Things Journal* 2019; 6(3): 4556–4560.

92. Yong Y, Yao D, Zhiqiang Z, Wei J, Shaoyong G. Edge Computing-Based Tasks Offloading and Block Caching for Mobile Blockchain. *Computers, Materials & Continua* 2020; 62(2): 905–915.

93. Fernández-Caramés TM, Fraga-Lamas P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* 2018; 6: 32979–33001.

94. Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems* 2018; 88: 173–190.

95. Hakak S, Khan WZ, Gilkar GA, Imran M, Guizani N. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Network* 2020; 34(1): 8–14.

96. Le Nguyen B, Lydia EL, Elhoseny M, et al. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. *Computers, Materials & Continua* 2020; 65(1): 87–107.

97. Le Nguyen B, Lydia EL, Elhoseny M, et al. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. *Computers, Materials & Continua* 2020; 65(1): 87–107.

98. Miller D. Blockchain and the internet of things in the industrial sector. *IT Professional* 2018; 20(3): 15–18.

99. Cao B, Wang X, Zhang W, Song H, Lv Z. A Many-Objective Optimization Model of Industrial Internet of Things Based on Private Blockchain. *IEEE Network* 2020; 34(5): 78–83.

100. Alladi T, Chamola V, Rodrigues JJ, Kozlov SA. Blockchain in smart grids: A review on different use cases. *Sensors* 2019; 19(22): 4862.

101. Ai S, Hu D, Zhang T, Jiang Y, Rong C, Cao J. Blockchain based Power Transaction Asynchronous Settlement System. *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*: 1–6.

102. Lombardi F, Aniello L, De Angelis S, Margheri A, Sassone V. A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids. 2018.

103. Amanullah MA, Habeeb RAA, Nasaruddin FH, et al. Deep learning and big data technologies for IoT security. *Computer Communications* 2020; 151: 495–517.

104. Chen J, Lv Z, Song H. Design of personnel big data management system based on blockchain. *Future Generation Computer Systems* 2019; 101: 1122–1129.

105. Transaction CP, MPI MPI. Blockchain: Opportunities for health care. *CP Transaction* 2016.

106. Bocek T, Rodrigues BB, Strasser T, Stiller B. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. *2017 IFIP/IEEE symposium on integrated network and service management (IM)*: 772–777.

107. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems* 2018; 42(7): 130.

108. Liu C, Li K, Tang Z, Li K. Bargaining game-based scheduling for performance guarantees in cloud computing. *ACM Transactions on Modeling and Performance Evaluation of Computing Systems (TOMPECS)* 2018; 3(1): 1–25.

109. Wan J, Li J, Imran M, Li D, others . A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Transactions on Industrial Informatics* 2019; 15(6): 3652–3660.

110. Xie S, Zheng Z, Chen W, Wu J, Dai HN, Imran M. Blockchain for cloud exchange: A survey. *Computers & Electrical Engineering* 2020; 81: 106526.

111. Dey S, Sampalli S, Ye Q. A context-adaptive security framework for mobile cloud computing. : 89–95.

112. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access* 2019; 7: 82721–82743.

113. Zhang Y, Deng R, Liu X, Zheng D. Outsourcing service fair payment based on blockchain and its applications in cloud computing. *IEEE Transactions on Services Computing* 2018.

114. Karamitsos I, Papadaki M, Al Barghuthi NB. Design of the blockchain smart contract: A use case for real estate. *Journal of Information Security* 2018; 9(3): 177–190.

115. Spielman A. *Blockchain: digitally rebuilding the real estate industry*. PhD thesis. Massachusetts Institute of Technology, 2016.

116. Mainelli M, Milne A. The impact and potential of blockchain on the securities transaction lifecycle. 2016.

117. Leinonen H. Decentralised blockchained and centralised real-time payment ledgers: Development trends and basic requirements. In: Springer. 2016 (pp. 236–261).

118. Salah K, Nizamuddin N, Jayaraman R, Omar M. Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access* 2019; 7: 73295–73305.

119. Wu HT, Tsai CW. An intelligent agriculture network security system based on private blockchains. *Journal of Communications and Networks* 2019; 21(5): 503–508.

120. Alvarenga ID, Rebello GA, Duarte OCM. Securing configuration management and migration of virtual network functions using blockchain. *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*: 1–9.

121. Brousmiche KL, Durand A, Heno T, Poulain C, Dalmieres A, Hamida EB. Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain. : 1281–1286.

122. Hassija V, Gupta V, Garg S, Chamola V. Traffic Jam Probability Estimation Based on Blockchain and Deep Neural Networks. *IEEE Transactions on Intelligent Transportation Systems* 2020.

123. Singh G, Singh A, Singh M, Sharma S, Kumar N, Choo KKR. BloCkEd: Blockchain-based Secure Data Processing Framework in Edge Envisioned V2X Environment. *IEEE Transactions on Vehicular Technology* 2020.

124. Bai S, Yang G, Rong C, Liu G, Dai H. QHSE: An efficient privacy-preserving scheme for blockchain-based transactions. *Future Generation Computer Systems* 2020; 112: 930–944.

125. Li X, Mei Y, Gong J, Xiang F, Sun Z. A Blockchain Privacy Protection Scheme Based on Ring Signature. *IEEE Access* 2020; 8: 76765–76772.

126. Tian Y, Yuan J, Song H. Secure and Reliable Decentralized Truth Discovery Using Blockchain. *2019 IEEE Conference on Communications and Network Security (CNS)* 2019: 1–8.

127. Akhtar Z. From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild. *2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON)* 2019: 1-6. doi: 10.1109/UPCON47278.2019.8980029

128. Hassija V, Saxena V, Chamola V, Yu R. A parking slot allocation framework based on virtual voting and adaptive pricing algorithm. *IEEE Transactions on Vehicular Technology* 2020.

129. Živić N, Kadušić E, Kadušić K. Directed Acyclic Graph as Hashgraph: an Alternative DLT to Blockchains and Tangles. *2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH)* 2020: 1-4. doi: 10.1109/INFOTEH48170.2020.9066312

130. Cullen A, Ferraro P, King C, Shorten R. On the Resilience of DAG-Based Distributed Ledgers in IoT Applications. *IEEE Internet of Things Journal* 2020; 7(8): 7112-7122. doi: 10.1109/JIOT.2020.2983401

131. Bartolomeu PC, Vieira E, Ferreira J. Pay as You Go: A Generic Crypto Tolling Architecture. *IEEE Access* 2020; 8: 196212-196222. doi: 10.1109/ACCESS.2020.3034299

132. Hassija V, Chamola V, Zeadally S. BitFund: A Blockchain-based Crowd Funding Platform for Future Smart and Connected Nation. *Sustainable Cities and Society* 2020: 102145.

133. Hassija V, Saxena V, Chamola V. Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory. *Computer Communications* 2020; 149: 51–61.

134. Deimel M, Frentrup M, Theuvsen L. Transparency in food supply chains: empirical results from German pig and dairy production. *Journal on Chain and Network Science* 2008; 8(1): 21–32.

135. O'Leary DE. Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. *Intelligent Systems in Accounting, Finance and Management* 2017; 24(4): 138–147.

136. Li X, Lv F, Xiang F, Sun Z, Sun Z. Research on Key Technologies of Logistics Information Traceability Model Based on Consortium Chain. *IEEE Access* 2020; 8: 69754–69762.

137. Hassija V, Chamola V, Gupta V, Jain S, Guizani N. A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal* 2020.

138. Sylvester G. *E-agriculture in Action: Blockchain for Agriculture: Opportunities and Challenges*. International Telecommunication Union . 2019.

139. Alladi T, Chamola V, Sahu N, Guizani M. Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications* 2020: 100249.

140. Hassija V, Chamola V, Krishna DNG, Guizani M. A distributed framework for energy trading between uavs and charging stations for critical applications. *IEEE Transactions on Vehicular Technology* 2020; 69(5): 5391–5402.

141. Chamola V, Hassija V, Gupta V, Guizani M. A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. *IEEE Access* 2020; 8: 90225–90265.

142. Alladi T, Chamola V, Sahu N, Guizani M. Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications* 2020: 100249.

143. Liu Y, Wang J, Song H, Li J, Yuan J. Blockchain-based Secure Routing Strategy for Airborne Mesh Networks. : 56–61.

144. Khalilov MCK, Levi A. A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials* 2018; 20(3): 2543–2585.

145. Hileman G, Rauchs M. Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance* 2017; 33: 33–113.

146. Li K. *The Blockchain Scalability Problem the Race for Visa-Like Transaction Speed*. Available at https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44#:~:text=Visa%20does%20around%201%2C700%20transactions,150%20million%20transactions%20per%20day).

147. *visa-net-booklet*. . Available at https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/visa-net-booklet.pdf.

148. Zhang X, Wu F, Yao W, Wang W, Zheng Z. Post-Quantum Blockchain over Lattice. *Computers, Materials & Continua* 2020; 63(2): 845–859.

149. page f. t. aET. *How a quantum computer could break 2048-bit RSA encryption in 8 hours*. Available at https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.

150. Aggarwal D, Brennen GK, Lee T, Santha M, Tomamichel M. Quantum attacks on Bitcoin, and how to protect against them. *arXiv preprint arXiv:1710.10377* 2017.

151. Gao YL, Chen XB, Chen YL, Sun Y, Niu XX, Yang YX. A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access* 2018; 6: 27205–27213.

152. Fedorov AK, Kiktenko EO, Lvovsky AI. Quantum computers put blockchain security at risk. 2018.

153. Ikeda K. Security and privacy of blockchain and quantum computation. In: . 111. Elsevier. 2018 (pp. 199–228).

154. Rodenburg B, Pappas SP. Blockchain and quantum computing. *Retrieved from* 2017.

155. Kim S, Kwon Y, Cho S. A survey of scalability solutions on blockchain. : 1204–1207.

156. Liu Z, Luong NC, Wang W, et al. A survey on blockchain: a game theoretical perspective. *IEEE Access* 2019; 7: 47615–47643.

157. Hassija V, Chamola V, Han G, Rodrigues JJ, Guizani M. Dagiov: A framework for vehicle to vehicle communication using directed acyclic graph and game theory. *IEEE Transactions on Vehicular Technology* 2020; 69(4): 4182–4191.