Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2021 SCPE. Volume 22, Issues 3, pp. 321–345, DOI 10.12694:/scpe.v22i3.1853

MOVING BEYOND THE CRYPTO-CURRENCY SUCCESS OF BLOCKCHAIN: A SYSTEMATIC SURVEY

MIR SHAHNAWAZ AHMAD* AND SHAHID MEHRAJ SHAH†

Abstract. Blockchain (BC) is a technology whose value today is estimated by the success of Bitcoin. However, the spectrum of Blockchain applications goes beyond the financial sector. It has displayed enormous potential for revamping the customary industry with its key merits like decentralization, persistency, anonymity, and auditability. In this paper we conduct a comprehensive survey on the blockchain technology, explaining its structure and functioning. This work has analyzed the potential of BC in seven crucial sectors vis. voting systems, supply chain management, the security of Internet of Things (IoT), healthcare, intelligent transportation systems, government services, and tourism. Moreover, this paper has critically evaluated the traditional technologies used in various sectors, the problems in them, and the benefits that will be provided by the employment of BC. With its future directions, this paper will help researchers to create and realize new value for various sectors that is beyond anything we can imagine with existing technologies.

Key words: Blockchain, Bitcoin, Decentralization, voting systems, intelligent transportation systems, security of Internet of Things (IoT) and government services.

AMS subject classifications. 68M25

1. Introduction.

A mixture of technologies like Artificial Intelligence, Internet of Things (IoT), robotics, cloud Computing, and Blockchain is marking the dawn of a new era in the world of information technology. Among these, BC is particularly noteworthy for its contribution in the creation of a strong backbone for decentralized data processing technology [1]. Although, originally conceived as the cardinal framework of the first cryptocurrency, i.e., Bitcoin, BC has cruised its way through the financial sector into a broad spectrum of applications, most of which are identified in this paper. Today, Bitcoin is identified as one of the most paradigmatic utilizations of Blockchain. Recognized as a famous substitute to fiat money, it is appreciated for its anonymity [2]. The users of Bitcoin are identified through cryptographic pseudonyms [3] and as long as the attacker's power of computation does not exceed that of the honest nodes in the network, the Bitcoin ledger has reliable liveness and consistency features [4]. Blockchain technology created this reputation of Bitcoin by being an immutable ledger that is secured by a network of peer-peer participants [5]. US Treasury identifies Bitcoin as a decentralized peer-peer virtual digital currency [6]. After the creation of Bitcoin in the year 2009, about 200 more crypto-currencies referred to as alt-coins were developed. Although these currencies were built by branching out from the original Bitcoin protocol, they do have their unique characteristics which make them different. Figure 1.1 lists various crypto-currencies as per their market capitalization values [7].

As per [7], the total market cap in digital currencies was approximated at 242 billion USD on 18th January 2020. With the present market value of 3,964 USD per unit of Bitcoin (bitcoin) and a total market cap of 68 billion USD, Bitcoin takes a 52% share of the whole market cap and ranks number one among all the crypto-currencies available today [8]. Figure 1.1 also demonstrates that the second and third largest digital currencies according to their market values are the Ethereum, and Ripple/XRP accounting for 12% and 10% capitalization values. Other currencies form the remaining 22% of the market capitalization value.

The decentralized nature of BC attract the attention of IoT, Supply Chain Management (SCM), Voting and multitude of other environments fitted out with decentralized topologies [9, 10]. Moreover, the distributed

*Communication Control & Learning Lab, Department of Electronics & Communication Engineering, National Institute of Technology, Srinagar, J&K, India. (mirshahnawaz888@gmail.com).

†Communication Control & Learning Lab, Department of Electronics & Communication Engineering, National Institute of Technology, Srinagar, J&K, India.

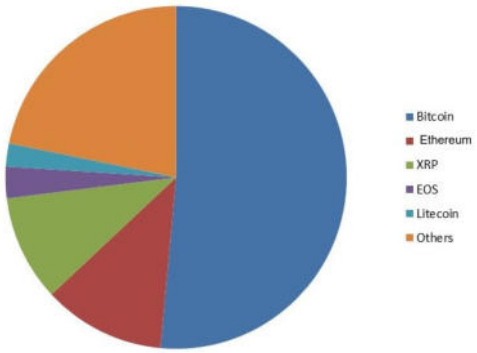

Fig. 1.1: Crypto-currencies by their market capitalization values.

consensus mechanism offered by the BC networks makes it crucial in the organization of global state machine for general purpose byte-code execution [11]. The consensus mechanisms used in BC offer concession that requires very less messaging overhead and absolutely no identification authentication on the global BC-data state. In addition to these reasons, since, BC can offer transaction driven asset management in communication networks, it is considered as one technology that can become the strength of developing trusted open-access virtual computers [12].

Although, a lot of potential areas concerning BC and research gaps in them have been identified in this paper, the key obstacle, however, in the path of true realization of BC in real business environments is that of the scalability [13]. Firstly, compared to the 2000 transactions per second carried by the VISA system, the Bitcoin system can only handle 7 transactions per second [3] and hence gives less throughput. Also, the block interval time is nearly 10 minutes and the number of transactions is limited by the size of the block which is 1 megabyte (MB). In real world, however, the number of transactions emerging is huge, and hence efficient schemes need to be built for BC to enhance its scalability and throughput. Secondly, the entire process of blockchaining consumes a lot of network resources because each transaction needs to be transmitted to all the nodes twice, first, when it is generated and second when it is mined. This not only wastes the network resources, but also increases block propagation delay. Thirdly, in BC, it is required that any node that processes the transaction stores it back to the genesis block. This makes it difficult to directly implement BC in environments where the nodes have limited computational and memory resources [14].

The main contribution of this paper is highlighted as follows:

- There is an adequate amount of literature on BC from diverse outlets, such as forums, wikis, forum articles, documents, conference proceedings, and journal papers. However, most of these scientific studies (discussed in the paper) revolve around decentralized digital currencies, including Bitcoin. Our paper, instead, focuses on the wholesome aspect of the BC technology, viewing it from both technological and application outlooks.
- Our work has organized the literature according to its categorization. It has compared the advantages of using BC technology over the ones that are currently being used.
- Our survey protocol is that first we have identified the fields where BC could be used apart from crypto-currencies, then we have reviewed the work done in that field, critically reviewing it and providing BC based solutions. As such, this paper can act as a guiding torch to the researchers for identifying the gaps and limitations in the existing work in various domains and direct them in how BC could be helpful.
- The IoT attack surfaces have also been explored in this paper. It also speaks how and where BC can help to mitigate this buzzing problem.
- Future research directions are collated for effective integration of Blockchain into various networks.

The rest of the paper is organized as follows: section 2 describes all the basic features of BC and its functioning. This section lays down the foundation for understanding the BC. Section 3 analyzes the areas

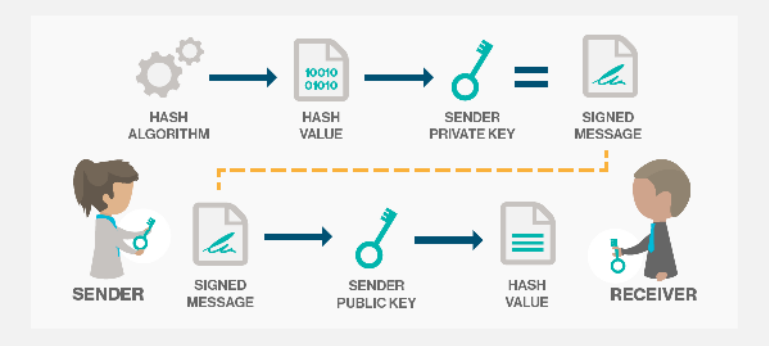

Fig. 2.1: Digital Signature in a Peer-Peer Network.

of voting systems, supply chain management, the security of Internet of Things (IoT), healthcare, intelligent transportation systems, government services and tourism from the viewpoint of BC, and sketches out the research directions in each of these fields. This section forms the major contribution of this article, describing the benefits of using BC in different fields where till date; otherwise, only the traditional technologies were used. Section 4 discusses various challenges that are posed in the way of implementing Blockchain technology in various fields. Finally, section 5 concludes the paper and identifies the research opportunities arising from the challenges in BC.

2. Basic features and functioning of Blockchain. A BC is a distributed, decentralized, shared and an immutable database that holds an encrypted ledger to keep the people involved in it completely anonymous. The fundamental building blocks of BC and their functioning is explained in the following sub-sections:

2.1. Block. It is a collection of all the recent verified transactions. All the transaction details are grouped, and their hash codes are created. These transaction groups along with hash codes are stored in a block. This hash code acts as a specific identification mark for the block. For every verified transaction, a block is permanently added to the BC.

2.2. Miner. Miners are elected as per the consensus algorithms discussed in subsection 2.6, and their job is to verify if a person like James has enough money to transfer. Valid transactions are time-stamped, ordered and packed into blocks [15]. Miners own what are called the supercomputer and solve complex puzzles. For performing their duties, they invest their energy and resources. For their effort every time they solve a puzzle, they get rewarded by the system.

2.3. Peer-Peer (P2P) network. The first thing that is needed to use a BC is a P2P network that ensures complete consistency concerning the BC. In a P2P network, every node gets two keys: the public key and a private key. Nodes sign a transaction using their private keys which ensure authentication, integrity, and non-repudiation; this is explained in figure 2.1. Verification of the received signed transactions are carried out by the peers before they broadcast it further into the network. Public keys, on the other hand, are used to encrypt data which can be decrypted only by the node that has got a unique private key. Hence, there is no scope of fraud in a distributed P2P network.

2.4. Blockchain Types. The type of BC is decided based on its accessibility and permissions available to the user. As a result, currently, BCs are divided amongst public, private and consortium types. Each of the kinds could be open (permission-less) or restricted (permissioned) and are described as:

- *Permission-less Public BC:* Ledgers are visible to everyone on the internet; anyone can join the BC, verify and add a block of transactions to it without requiring an approval from any third party/ validator/ miner. Public BCs are most often open and include examples like Ethereum, Bitcoin, and Litecoin [16].

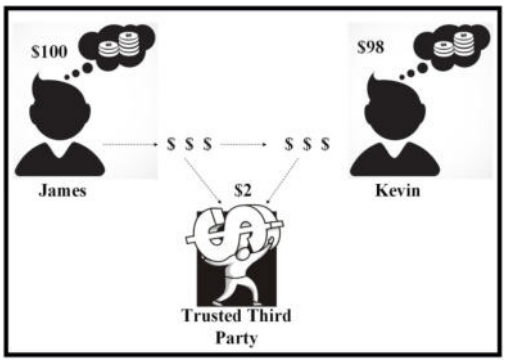

Fig. 2.2: High Transaction fees.

- *Permissioned Private BC:* Only specific individuals from an organization are allowed to verify and add transaction blocks. However, everyone on the internet is generally allowed to view it. Ripple [17] and Hyper-ledger [18] form the typical examples of permissioned private BCs.
- *Consortium BC:* A mix of public and private BCs which allows a group of organizations to verify and add transactions to blocks. The ledger here is either open or restricted to the select groups.

Christine et al. [19] provides a detailed analysis of various barriers and drivers of diffusion related to permissioned and permission-less blockchains using a case study of the Italian wine industry. They also highlight various application domains based on the unique characteristics/ properties of each type of blockchain and how the applications of blockchain can be further enhanced by diffusing permissioned and permissionless blockchains.

2.5. Hash Function used. Secure Hash Algorithm SHA-256D employed by crypto-currencies like Bitcoin and Namecoin, SHA-256 used by Ethereum, and Scrypt utilized by Litecoin, and Dogecoin represent the most famous of all the hash functions employed in BC applications.

2.6. Algorithms used. A lot of algorithms are needed for the proper functioning of a BC. Various cryptographic algorithms, time-stamping algorithms, consensus, validation and mining algorithms are used by the BC to suit the requirements of different applications.

- *Cryptographic algorithms:* The commonly used cryptographic algorithms in BC include RSA and Elliptic-Curve Diffie-Hellman Key Exchange. They guarantee strong encryption of the ledger for maintaining the anonymity of the users [20].
- *Time-stamping algorithms:* Transactions need to be time-stamped to track changes on the BC. For this purpose, time-stamping mechanisms have to be used. Bitcoin, for example, uses the procedure offered in [21], where the transaction order is maintained by having every timestamp to include the last time-stamps hash code. The procedure makes it hard to add fraudulent transactions to the chain. Other mechanisms used in other crypto-currencies include the ones essayed by the authors of [22, 23].
- *Consensus mechanisms:* Consensus ensures the apt working of BC by making it possible to establish the ultimate truth about the transaction histories. Consensus mechanism refers to the procedure that decides what conditions need to be met so as to presume that an understanding has been reached in respect to the validation/approval of the blocks to be added to the BC [24]. In other words, they help the transactions to be confirmed without depending on a bank or any other third party.

Some of the consensus mechanisms used in BC are listed in table 2.1.

2.7. Basic Financial issues tackled by Bitcoin. Banking systems suffer from major issues like varying interest rates, high transaction fees (figure 2.2) and double spending. Peer-peer doubling spending was such a huge problem that it became the motivation for the development of Bitcoin technology [33]. Current banking systems are prone to double spending where a person can spend an amount two times. Figure 2.3 explains the problem.

Table 2.1: Consensus Mechanisms used in BC.

Consensus Mechanism	**Description**	**Highlights**	**Drawbacks**
Proof of Work based BC (POW-BC)	Assumes that if some node is performing a lot of work for the network, there is less probability that it will attack the network, e.g., miners [15].	Sybil attacks cannot be carried out in POW-BC because the attacker will have to perform extensive computations for forging the identity. These computations are not only complex but also expensive to be carried out by a single individual [25]. Used by Ethereum.	Miners need to prove they are doing work. POW-BCs have fewer through- puts, are expensive, have less scalability, and consume high energy. Are prone to be attacked by miners because they gain dominance [25].
Proof of Stake based BC (POS-BC)[26]	It considers the nodes with greater stake/currency in the network to be the least prying about attacking it [15].	Needs less computation power than POW and utilizes less energy.Requires less hardware. Highest stakeholders validate and create the blocks.	The richest rule the BC, hence unfair. Rich with a motive to destruct the system can do so.
Delegated Proof of Stake based BC (DPOS-BC)	Instead of stakeholders, delegates are chosen to perform generation and validation of blocks [27].	Quicker transactions because lesser nodes perform validation tasks. Any misbehavior by delegates leads to their substitution. Election of delegates brings democracy into the system.	Ownership still rules. Organization of attack is easier because only a few delegates who control the network need to be compromised.
Transactions as proof of stake based BC (TaPOS-BC)	Nodes responsible for the generation of a transaction contribute to network for security [28].	Enhanced network security. All the nodes and not only the bigger stakeholders take part in the consensus.	Requires more hardware and more complexity. More computational energy required.
Proof of Activity based BC (POA-BC)	The validator in all of the POS variations has all the power to commit the crime of double spending. POA is a hybrid consensus algorithm comprising of features from both POW and POS [29].	Unlike POS-BCs that increase the status of nodes which are not even connected to the network, it limits the status if the node does not connect. It rewards only those stakeholders that take part in the network activities. Prevents chances of attack.	Extra power consumption from POW. Ownership problems from POS.
Practical Byzantine Fault Tolerance based BC (PBFT-BC)	It tries to solve the popular Byzantine general problem, explained as the problem of knowing that all the entities allowed to take action are in full agreement before they do so [30]. PBFT considers that not more than 1/3rd of nodes in BC can be nefarious [30].	Selects leaders for each transaction, a selection which is agreed upon by a minimum 2/3rd of all the nodes. Democracy in selection. The block becomes final when nodes in the PBFT system agree upon it. Less energy consumption as compared to POW.	Susceptible to Sybil attacks. High communication complexity of $O(n^2)$.
Ripple based BC	The iterative procedure meant for maintaining the agreement correctness of the network. Transactions are pushed forward in batches to all the other nodes when almost 50% of nodes approve the transaction [31]. Transactions are written on the ledger only when 80% of the nodes approve it [31].	Less latency, attack tolerant, less energy intensive.	List to who you want to reach in consensus with must be maintained properly and if they are broken you will fail in various ways. Ripple is path dependent, i.e., it memorizes the past which increases its memory complexity to maintain the chain.
Tendermint based BC	Bears only up to 1/3rd of the failures, i.e., a block can be passed only if 2/3rd of the validators/BC participants pre-commit it in one round [32].	With the assumption that no more than 1/3rd of validators can be byzantine, Tendermint assures safety. Provable liveliness in a partially synchronous network. Instant finality of 1-3 seconds.	Communication complexity is the same as that of ripple, i.e.,$O(n^2)$. When the tolerance threshold increases, things start to blow up.

Figure 2.2 shows that the third party takes heavy transaction fees of $2 out of the total $100. Also, it is clear from figure 2.3 that without verification from the bank or some other central intermediary there is no way Kevin can know if James has sent the same amount to Paul as well. Bitcoin solves these issues by having:

- *Decentralized Power:* Bitcoin makes any individual entering into the system a very powerful person. When a transaction happens, its information gets broadcasted to all the people that form the BC network or as they say in [34] "Everyone sees everything". As such, the power is distributed and not centralized like banks, which alleviates the problem of single-point-of-failure. The single-point-of failure node is the one which if goes down takes the entire system with it and if it gets hacked, the entire network is exposed to danger.
- *Immutable Transactions:* Financial organizations are prone to assaults. Since BC transactions are immutable and the ledger is encrypted, transactions in BC are secure and valid, if successful [16].

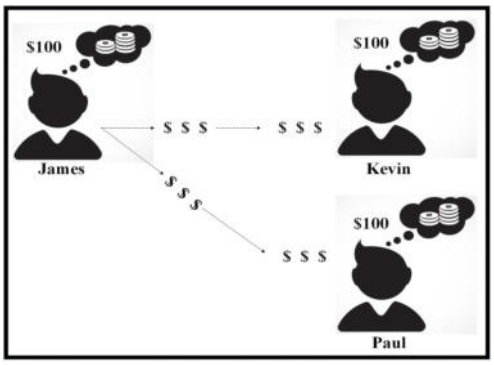

Fig. 2.3: Doubling spending problem.

If a hacker attempts to modify even a single transaction detail, its request gets rejected because everyone in the network has an updated and a valid copy of the block. Consequently, if James sends $100 to Kevin today and then tries to send the same $100 to Paul tomorrow, the transaction will be rejected without having to consult any central intermediary like a bank.

3. Applications of Blockchain in sectors other than Finance. The use of BC outside finance is still in the experimental phase. Some of the most promising non-finance applications of BC include:

1. Voting System.
2. Supply Chain Management.
3. Internet of Things (IoT) Security.
4. Healthcare.
5. Intelligent Transportation System (ITS).
6. Government services
7. Tourism.

These regions are seemingly solid fits for BC. To properly reckon the advantages of using BC in these fields, we analyze the contemporary technologies that are used instead of BC in these areas. These are explained in the following sub-sections.

3.1. Voting System. One of the central pillars of modern democracy is voting [35]. The success of a democracy relies on the level of fairness and reliability of its elections. Electronic voting machine (EVM) tampering allegations and electoral frauds (like inaccurate or invalid votes, multiple registrations, etc.) always surface whenever there is an election season in various countries. This happens because EVM' s suffer from substantial weaknesses like [36]:

- Absence of transparency and auditability of the system.
- Lack of understanding of the system which prompts loss of trust and undermines its entire sense.
- Absence of widely acknowledged standards in voting systems.
- Danger of tampering and fraud by insiders.
- Increased expenses of ballot infrastructure in terms of power supply, communication technology, etc.
- Use of malicious hardware and software [37]. The elections could be maneuvered in the favor of a particular candidate by using techniques like replacing the circuit board with a look-alike, manipulation of the memory unit or manipulating stored votes by vote stealing attacks remotely, etc.

How BC can help: Blockchain-based voting system will bring the following key benefits in voting systems:

- Blockchain-based voting system shall bring auditability to the voter level, i.e., instead of insider officials and specific organizations, voters themselves would be able to audit the e-voting system.
- The voting scheme will have the properties of decentralization and self-management as well. This shall reduce the expense [38].
- The Blockchain voting system will also improve the security of voting; any break-ins into the voting

system can be detected easily.

- Blockchain-based voting systems solve the multiple-vote registration problem by offering only one "votecoin" to an individual who uses his/her private key to access his/her voting right and public key to choose his/her preference. Once this votecoin is exhausted, the vote will be registered in the system after verification by all the blockchain stakeholders. Hence no more voting can be performed by the individual [38].

Literature survey on current work: This sub-section highlights the current work being done on blockchain voting, as well as the progress and challenges of this widespread adoption.

Blockchain based voting frameworks are proposed in numerous papers [39],[40]. [39], proposes a blockchain architecture that advocates a different blockchain to each applicant taking part in the election.

In [40], to improve the security level asymmetric encryption utilizing RSA is performed on the information before it is put in the blockchain. In [41], an E-Voting framework is created utilizing smart contracts. It additionally assesses three diverse blockchain structures, Exonum, Quorum and Go-Ethereum, dependent on how reasonable they are for an E-Voting framework.

Application specific e-voting frameworks utilizing blockchain are additionally proposed in [42], [43]. In [25], a PIN based scheme is used for authentication that is utilized to check the voters and empower them to check their votes after the election process is over. Two distinct Blockchains are utilized to record the votes and the voter IDs of the voters who had made their choice. In [27], a centralized Authentication Server (AS) is utilized to check the voters, and a decentralized, blockchain based Arbitration Server (AR) is utilized to store the votes. BronchoVote [44] is a web-based platform that uses Ethereum Blockchain technology and smart contracts to provide authentication, anonymity and voter verification benefits in e-voting. BroncoVote has been implemented on a university scale. It has also worked on to achieve the voter privacy by making use of homomorphic encryption. Similarly, [45] uses Zerocoin to enhance the anonymity of voters. However, when critically analyzed, [45] has the tendency for centralization and it does not handle exceptions.

[46] presents Shamir secret sharing approach for giving a new definition to cryptic e-voting by using the Blockchain technology. It does not require any middleman to improve the voting processes of auditability and traceability.

Other recent research works include university projects like Voteboook (New York University) [47], Vote-Watcher [48], Openvotebook network (New Castle University), and the proposal of university of maryland [43]. A common limitation of crypto-currency based systems, however, is they are very volatile [49]. A huge monetary risk is involved for the organizer. Tassos Dimitriou [50] has proposed a universally verifiable secure blackchain based voting system with least computational and communication overhead on the voter. The system makes use of a randomizer token (black box representing a voter) for achieving security for each voter. To make the system more secure, author proposes to use a consortium blockchain for the implementation of a bulletin board, but this would require the intervention of impartial observers, thus increasing the overall computational complexity of the system and dependence on third party.

3.2. Supply Chain Management (SCM). The supply chain can range over numerous vertical stages, several horizontal connections, different geological areas, varied financial frameworks, various individual characters and elements included, and with changing chronological stresses relying upon the item and market. These measurements are hard to oversee and normally all the better we can do is make them at first powerful and effective with consistent improvement as an objective [51].

The primal objectives of SCM include the optimal quality, less cost, better speed, risk reduction, dependability, transparency, accountability, sustainability, and flexibility [53]. SCM has taken advantage from another famous paradigm called Internet of Things to achieve these objectives and righteously so IoT did transform this sector by helping in the identification, and tracking of goods using sensors, Radio Frequency Identification (RFID) tags, Global Positioning System (GPS) tags, barcodes, and chips. Nonetheless, it suffers from a lot of problems in identity management, and governance of these goods. The challenges include:

- *Ownership and Identity of IoT devices:* In its lifetime, a device moves from the ownership of a manufacturer to a supplier and then from supplier to a retailer and finally into the dominion of a consumer. Furthermore, if the device is compromised, decommissioned or resold, then the consumer ownership gets either revoked or changed [54].

- *Attribute and Relationship Management of IoT devices:* Attributes of a device can include the manufacturer name, its make, the type, serial number, deployment GPS coordinates, location, etc. In addition to these attributes, they have relationships. IoT relationships may include device-human, device-device, or device-service. The examples of IoT device relationships may include relationships like deployed-by, used-by, shipped-by, sold-by, upgraded-by, repaired-by, sold-by, etc. [55].

Employment of blockchain can easily and securely deal with these challenges with its reliable and authenticated identity management. It can ascertain "who is doing what" and at what time is s/he doing that [56]. The other advantages that blockchain technology can bring into SCM include:

- *Better Performance and Trust Evaluation:* BC technology can effectively and validly measure the results obtained, and evaluate the performance of the SCM process. The moment any SCM input data finds its place on the BC distributed ledger; there is no way it can be changed, i.e., it is immutable. This brings trust among suppliers. The BC procedure also eliminates auditors implying reduction in costs, and increase in efficiency. The suppliers can perform checks on their own processes in real-time [57].
- *Assessment of Quality of Product during its Transportation:* BC solutions can be used to assess the travel duration and paths which can help in assuring the quality of the product. For example, products that require refrigeration must not be held in warm conditions for a long duration. If that happens, their quality is compromised [53]. The BC solutions, therefore, give a sense of security to the consumers who use the products.
- Blockchain advocates transparency, speed, openness and non-falsifiability as the foundations of this new worldview. Blockchain innovation can make it significantly more difficult, if not completely impossible, for unlawful or fake items, for instance, adultered or infringing excipients, or merchandise whose processing is naturally unfavorable to enter authentic inventory chains. It would empower end clients to confirm precisely how, where and by whom the item they plan to buy has been gathered and made, accordingly denying a business opportunity for unlawful and fake items [57].

Literature survey on current work: [51] identified the top motivators and barriers to the adoption of BC technology in SCM. It identifies organizational barriers (lack of knowledge on BC, and dearth of tools and standards to implement BC.), supply-chain linked barriers (paucity of end-user awareness regarding BC technology, lack of supply chain partner collaboration and coordination.), technological (infancy of the technology itself and finite available infrastructure) and external barriers (uncertainty on how market will respond to BC adoption, lack of involvement of industry in BC adoption) as the four major categories of barriers to BC adoption in SCM. It also identified reducing operation cost, increased security and improved information traceability as the top drivers of BC adoption in SCM.

In their work, Mattila et al. [52] investigated the chances of utilizing blockchain to help product-centric information management so as to give an effective engineering to gather information on items over their whole life-cycle. The consolidated utilization of RFID and blockchain is additionally investigated by [58], to empower track and tracking of items in the Chinese agri-food market to upgrade security and quality while decreasing food squander.

Start-ups are using BC for improving traceability [59]. For Instance, an industry partner Provenance started to work with Co-Op, a UK based retailer in 2016 to track fresh foods through its BC based supply chain. An agreement was signed between the enormous retail associations Wal-Mart, IBM, and Tsinghua University in October 2016 for investigating the chances of blockchain in food authentication and supply chain tracking. With this, in March 2017 Walmart became one of the 400 IBM customers testing blockchain innovation. One more striking example of the industry initiative is by the company called Modum.Io (a pilot project initiated in June 2016). The motivation for this project is the monitoring of humidity and temperature measurements of the medical items that do not require refrigeration during their transportation. This information is transferred to the Ethereum BC upon reaching the destination.

Sara et al. in [60] provide a detailed analysis of data (regarding the use of blockchain by various companies) gathered from 173 companies of Association of Supply Chain Management (ASCM). The study helps to understand various barriers for the use of blockchain in supply chain management. The study concludes that there needs to be more expertise regarding the application of BC in supply chain management, increased

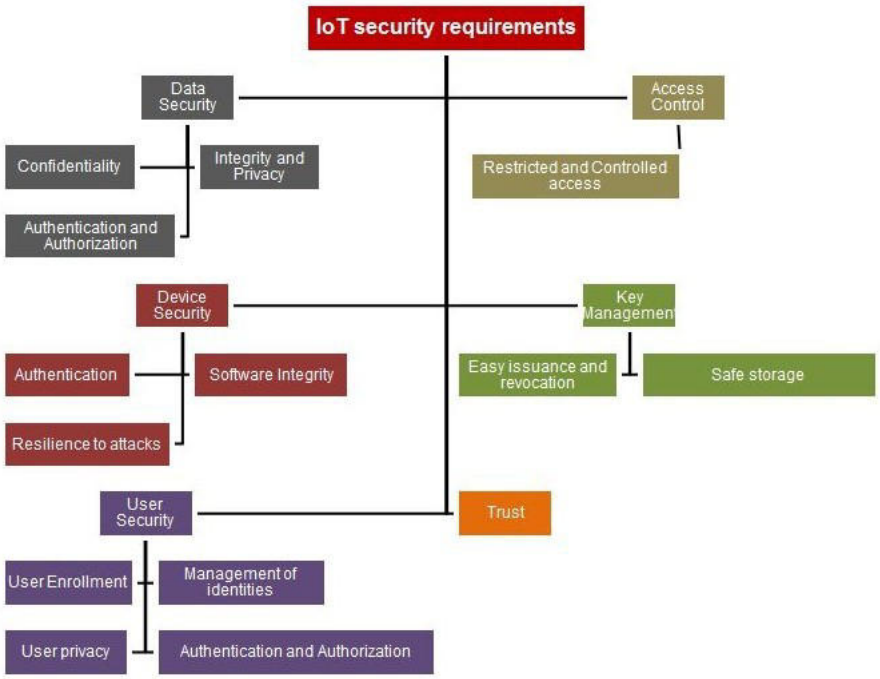

Fig. 3.1: IoT security requirements.

collaboration with the supply chain partners and enhancement of information security.

3.3. IoT Security. IoT is a technology that has revolutionized the world by offering services in almost all domains. On the other hand, presently, IoT devices suffer from a lot of Security and Privacy (S&P) issues.This is because the developers of IoT devices focused mainly on their tempting features and left their security as an afterthought [61]. BCs are computationally expensive and involve high bandwidth overhead, and delays, which are not suitable for IoT devices [5]. The security professionals from all around the world, however, are vouching on the BC to settle down these S&P issues for its peculiar benefits like decentralization, fault tolerance, pseudonymous identities, cryptographic security, authentication, and data integrity [62].

3.3.1. Security requirements for IoT and related work. The parameters that need to be taken care of for ensuring a secure IoT environment are summarized in figure 3.1. These requirements are described as under [55, 62].

- *Data Security:* Since there are no boundaries in IoT networks (data can travel through numerous hops), encrypting the data is extremely important to ensure confidentiality. The devices are highly vulnerable to attacks, and thus an attacker may modify the data to accomplish his/her heinous crimes thus compromising the integrity. Moreover, because of the huge diversity of devices and services, privacy violations could happen by compromising the devices present in the IoT network. To check the work done on the confidentiality in IoT using BC, one can refer to PriWatt [63], Axon et al. [64], Dorri et al. [5], [65], Hardjono et al. [66], IBM Hyperledger [67],[68], Munsing et al. [69], Neha et al. [70], Ouaddah et al. [71], Shafagh et al. [72], Tourancheau et al. [73],Guan et al. [74], Mettler [75]. End-end security, optimized for IoT data requirements is provided by a lightweight and scalable BC mechanism offered by the authors of [76]. This instantiation allows the nodes that have high resources to manage the network. The public blockchain is maintained by the cluster heads to make the system distributed.
- Authentication and authorization of the systems are equally important. While authentication spots "who is who?" authorization establishes "who can do what?" An IoT security mechanism must be

able to perform both. Given the huge number of available IoT architectures, it is crucial to ensure that a standard global protocol for authentication and authorization is established for IoT. Ghuli et al. [77], Hashemi et al. [78], Huh et al. [79], AuthCoin [80], IBM Hyperledger [67],[68], Wu et al. [81], English [82] have proposed various authentication and authorization techniques for IoT devices using Blockchain.

- *Access Control:* There is a whisker between access control and authorization. An Access Control System (ACS) makes sure that any specific node has all the essential requirements fulfilled for it to claim the right to be authorized. It certifies that a particular node falls within the bounds of a local network while as authorization assures that a node is good enough to access it. In [78], the authors have designed a system that allows users to give access to their data by issuing tokens. The Chain-anchor [66] architecture offers commissioning of the resource-constrained IoT devices into cloud systems using a permissioned Blockchain. [5],[65] also propose an access control mechanism for IoT devices by creating an access control list stored in the header of BC. Since, multiple parties like manufacturers, users, operating platforms, etc. are involved in IoT, it becomes imperative to establish a collaborative trust amongst all of them. This is made possible by the IoT passport framework proposed by the authors of [83]. IoT passport is a decentralized trust framework that includes BC based authorization, authentication, and trust as its foundation stones.
- *Device Security:* The devices used in any IoT environment are prone to be compromised as they are usually deployed in public places, and essentially lack the inherent capability to include security themselves. Hence, it is important to ensure device authentication, its software integrity, and its resistance to any hardware or software tampering. Jason and smart contract based security policy has been proposed in [84]. The authors of [61] have orchestrated a multi-faceted solution called Neuromesh to IoT device security using the Bitcoin protocol. Neuromesh is able to identify and remove any IoT device malware, and blacklist any suspicious IP address to allow secure communications.
- *Key Management:*Efficient key management is essential in IoT that allows safe storage, an easy revocation of compromised keys and updating of old ones as and when necessary. In [62], the researchers have proposed a scheme called "blockchain based distributed key management architecture (BDKMA)". It uses BC technology to fulfill the decentralization, auditability, and high scalability requirements, as well as the privacy-preserving principles for hierarchical access control in IoT.
- *Security of User:* User security is a pivotal requirement for establishing the holistic security of IoT networks. It shall include the identity management of users, their enrollments, authentication, authorization, and privacy. The security of user has been discussed in papers like [66],[85] and [86].
- *Trust:* All the nodes of the system should have a certain degree of trust on each other. This trust must be established both ways, i.e., a higher level node (fog/cloud node) must be sure that the device sending it the data or asking for its services is legitimate while as the IoT devices must also establish that the node (cloud/fog) to which they are sending their data is secure. The current work on BC in this field include PriWatt [63], Axon et al. [64], Bahga et al. [87], Herbert et al. [85], IBM Hyperledger [67],[68], Nehai et al. [70], Zhang et al. [86], English [82], Mettler [75].

3.3.2. Categories of IoT Security Issues. The security issues of IoT paradigm could be categorized into three levels: Low-level, medium-level and top-level security issues for the reason that these IoT devices range in their functionality, and size from simple processing chips to huge high-end server [55]. The IoT security issues are summarized in Table 3.1.

3.3.3. Blockchain Solutions to these Issues. IoT's security and privacy issues could be resolved by taking advantage of BC benefits listed in figure 3.2.

The decentralized operation of BC along with its immutability offers a perfect solution for IoT systems that operate in highly vulnerable environments [62]. In table 3.2, we explore the additional advantages that BC-based IoT architecture would bring to the IoT's S&P. It gives a comparison between cloud-based IoT systems and BC-based IoT systems.

Blockchain offers a 160-bit address space [108] and therefore can generate an address for almost $1.46 * 1048$ IoT devices. This reduces the address collision probability as it provides 4.3 billion addresses more than IPv6. This makes BC a more scalable solution for IoT than IPv6 [55]. Moreover, most of the attacks on IoT devices

Table 3.1: Security issues prevalent in IoT.

Security Issue	Level	Description	Reference
Jamming	Low	Wireless IoT devices are targeted by degrading the network. Jamming of channels is performed by emitting radio frequency signals without following any standard protocol.	[88, 89]
Insecure Initialization	Low	When the IoT network is not initialized properly at the hardware layer, privacy violation and disruption of various network services can happen.	[90, 91]
Sybil	Low	Sybil nodes are defined as the ones that use fake identities to bring down the functionality of a network. At this level, Sybil nodes deplete network resources and starve the legitimate devices from using them.	[92, 93]
Insecure Physical Interface	Low	If the software that gives physical interface is insecure, its weakness could be used to target nodes in the network.	[94]
Sleep Deprivation	Low	These attacks cause the IoT nodes to always remain in the "wake-up-state." This causes unnecessary battery drainage.	[95]
Replay Attack	Medium	IoT networks follow the 802.15.4 protocol which gives a Maximum Transmission Unit (MTU) of 127 bytes. This makes fragmentation of IPv6 packets mandatory. Their re-assembly consumes resources. Hence, if replay attacks are launched, extreme resource wastage can happen. Moreover, the processing of legitimate packets will be affected.	[96, 97]
Buffer Reservation Attack	Medium	For re-assembling the fragmented packets, the IoT receiver nodes maintain some buffer space. This attack depletes that space by sending incomplete packets leaving no space in the buffer for the actual ones.	[97]
Sink-hole Attack	Medium	The attacker node quickly responds to the routing requests for luring the sender to route all its packets through it. It then performs its malicious activities.	[98, 99]
Transport level end-end Security	Medium	It ensures that data is received in the exact form and shape by the receiver as sent by the sender.	[100, 101]
Session Management	Medium	If the transport layers session is hijacked, it can result in Denial of Service (DoS).	[102, 103]
Constrained Application Protocol (CoAP) Security with Internet	Top	CoAP is a web-transfer protocol which is vulnerable to a lot of attacks and therefore requires: Encryption for securing the communication. Efficient key-management and authentication procedures for its multicast support.	[104, 105]
Insecure Interface	Top	IoT services accessed through mobile, web, and cloud will be prone to multiple data privacy attacks if the interface is insecure.	[94]
Insecure Firmware	Top	The codes written in languages like TSON, XML, XSS, etc. require proper testing. The updates need to be performed securely.	[94]

Table 3.2: Advantages of BC over Cloud based IoT architectures

Comparison Parameter	Cloud IoT	Blockchain IoT
Architecture [62]	Centralized.	Decentralized.
Trust [106]	Put on the cloud.	Distributed in the network.
Existence of single-point-of-failure [107]	Yes.	No.
Mutation [34]	Data manipulation is possible.	It is immutable.
Data Sharing [62]	Un-authorized data sharing is possible.	Access control is user defined based on smart-contract technology.
Cost [62]	Expensive.	Less-expensive.
Transparency [62]	The Users have no idea about the way intra-cloud transmission happens.	An unforgeable log of transmissions and events is created and maintained.
Latency [55]	High latency, hence it is unsuitable for applications demanding quick responses.	Offers edge devices to store data and perform computations, hence producing quick responses.

are launched because of their memory and other resource constraints. Running an IPv6 stack becomes an additional liability.

Sybil and spoofing attacks are launched when the attackers use pseudo-identities. The creation of Sybil identities could be restricted only by the incorporation of a strong trust relationship [55]. There is an inherent trust in the BC because of its distributed power, and decentralized control. BC is typically popular for its reliable and authorized identity registration, ownership tracking, and monitoring of items [55].

Attacks on buffer and session managements could be prevented by blockchain's data authentication and integrity. The data sent by the IoT devices in a BC at all times remains encrypted as well as signed by the

Fig. 3.2: Blockchain for IoT

original sender, who holds a unique public key, and its unique identifier. The attacker can neither use his/her signature; nor can take anyone else's identity. Hence, these attacks could be avoided.

The protocols widely used in IoT environments like Routing Protocol for Low-Power and Lossy networks and IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) need a security wrap from other protocols such as DTLS and TLS for messaging because they are not inherently secure. Likewise, for routing RPL and 6LoWPAN need a wrapping from IPSec. All these protocols, i.e., DTLS, TLS, and IPsec are heavyweight and complex in terms of memory needs and computational requirements [55]. Their complication comes from the central management and governance of key management and distribution that uses the famous PKI protocol.

BC offers secure communication in the manner that it eliminates the need to have any key management and distribution procedures which bring up security issues in IoT networks. In BC, every IoT device gets an asymmetric key pair and a Global Unique Identifier. As such, the messaging protocols DTLS and TLS would not require the exchange of PKI certificates in the handshake phase.

3.4. Intelligent Transportation System (ITS). The manner in which the Internet of Vehicles (IoV) connects vehicles with each other and the Road Side Units (RSUs) brings peculiar security challenges into the picture [107]. The black-hats can hijack a vehicle, which can result in compromising passenger safety, endangerment of the public property and putting at-risk the life of others on the road [109]. For example, an attack was launched by the white-hats Miller and Valesek on the vehicle infotainment system to remotely control its functions [110]. Also, the vehicles share some critical information with each other which if hacked brings about privacy issues.

Table 3.3 analyzes the issues with the classical Security and Privacy (S&P) methods that are used in smart cars and why they remain ineffective to solve them. It also sketches out how BC can achieve the same purpose effectively.

Literature survey on current work: Ensuring the reliability of messages exchanged between vehicles is a major challenge in ITS. Motivated to address this concern, Yang et al. [111] designed a BC based distributed trust management scheme for ITS. Experimental results demonstrate that the proposed system is efficient and practical for facilitating trust in smart vehicular systems. Similarly, authors in [112] proposed a BC based system for ensuring secure and trusted communication between vehicles in ITS. Simulations show that the

Table 3.3: Comparison of Conventional and BC-based methods in Smart cars.

Parameter of Comparison	**Conventional S&P Approach**	**Benefits brought about by BC**
Architecture [107]	Centralized, and non-scalable.	Decentralized, and scalable.
Participation [107]	Partial, not all devices contribute to S&P.	End-End participation.
Privacy [109]	Lacks privacy. Driver's privacy can be at-risk because of a direct link between the vehicle, and the Original Equipment Manufacturer (OEM).	Privacy assured.
Verification of activities [107]	Performed by OEM	Events publicly verified.
Integrity [107]	Data exchange is insecure which compromises integrity.	Secure and privacy preserving exchange of data is ensured.
User control [107]	No control can be exercised by the user over the data exchange.	The user enjoys full control and transparency over data exchange.
Payments and accounting [109]	Centrally controlled.	Payments and accounting have distributed security, and happen privately.
Tracking of customer [109]	Both location and behavior could be tracked.	Information about location and behavior remains private.

Table 3.4: Comparison of traditional and BC-based methods in Healthcare.

Parameter	**Traditional Systems**	**BC Systems**
Management [118]	DDBMSs are intrinsically centrally managed. The applications requiring independent control over the repository cannot function.	Every node runs independently of others, i.e., they are decentralized. Gives full independence to applications.
Mutability of audit trail [119]	Traditional systems only offer functions like create, read, delete, and update which makes them prone to mutation attacks.	BC systems allow create and read functions, making them feasible for recording critical information that requires immutability. BC guarantees that nobody, neither a doctor nor the patient her/himself can change the records.
Data provenance [120],[121]	Administrators enjoy the power of shifting the ownership of digital assets. The assets cannot be traced, i.e., data records cannot be confirmed. No way to deny false records.	Only the owner can modify the ownership credentials and that too by following the standard cryptographic protocol. Assets can be traced. Records are always signed by the source. False records are denied.
Reliability [34]	No single-point-of-failure, since DDBMSs are distributed.	No single-point-of-failure.
Availability [34]	To maintain entire histories of records, DDBMSs become costly.	BC offers continuous access to and availability of data.
Security and Privacy [122], [123]	No security mechanism is employed. BC utilizes 256-bit Secure Hash Algorithm (SHA) for assuring anonymity and privacy. Here every user gets a unique hash value instead of an IP address.	BC uses 256-bit elliptic-curve-digital signature algorithm for ensuring data integrity in the form of digital systems.

study was able to resolve three major challenges: authentication, trust, and validation in ITS. In [113], authors designed a distributed framework for efficient key management in ITS. Simulations conducted in the study reveal that the proposed framework provides better flexibility than centralized Key Management Schemes. Dorri et al. [107] proposed a decentralized BC based architecture in order to ensure user privacy and safety of smart vehicular systems. Due to the privacy concerns in ITS, the users are reluctant to forward traffic announcements. To this purpose, the authors in [114] proposed CreditCoin, a BC based system that encourages the users to share their traffic information. Experiments carried out in the study demonstrate that the proposed system is efficient and easy to implement. Qilei et al. [115] designed a BC based ITS that gathers information about the traffic conditions and detects accidents. Cebe et al. [116] designed a BC based forensic framework called as Block4Forensic to resolve a dispute while investigating accidents. The framework resolves the dispute by involving the crucial factors like conditions of the road, details about manufacturing company and maintenance centers, other vehicles, etc. Performance analysis conducted in the work reveals that the framework is effective for dispute resolution. Rajat et al. [117] proposed a BC based framework for efficient and secure energy trading in electric vehicles. Performance evaluation carried out in the study demonstrates that the proposed framework is effective and resource-efficient.

3.5. Healthcare. Majority of the developed countries spend more than 10% of their GDP on their Healthcare systems [124].The systems that were traditionally used for healthcare applications include Distributed Database Management Systems like Oracle [125], and Apache Cassandra [126]. The key advantages offered by BC over these are tabulated in Table 3.4.

Moreover, the Blockchain offers solutions to contain all the properties that the health data of an individual must display. These include:

- Right from the time a person is born, his/her entire health, disease, and treatment information must be summed up in it. BC is an affordable gateway to store redundant information/histories of data which if recorded with any other technology becomes costly [34].
- The data must strictly adhere to the procedures of security like anonymity, confidentiality, integrity, etc. The BC is inherently designed for offering these security advantages [123].
- It must include only one instance of truth. Multiple instances of truth cannot exist in BC, as any record that finds its place in the distributed ledger of BC goes through a complicated verification procedure [120, 121]
- The down-time of this data must be zero.
- It must remain strong against attacks. BC is more secure in comparison to its contemporary technologies in healthcare [122, 123].
- It must rebound easily, i.e., if the owner loses her/his key, they must be able to make access to the same. BC data is always available [34]. Moreover, its transparency feature will allow for this rebound to happen quickly.
- The data must be ubiquitous. Public Blockchains will make the data ubiquitous.
- The views of health data should be distinct for different players.
- It should be immutable. The BC's foundation is laid on this feature [119]-[123].

Literature survey on current work: By designing a BC based healthcare data gateway, the authors of [119] have tried to mitigate the user privacy issues that arise in healthcare data. Privacy is the focal point of establish who and whom should be given access to patient's health data [127]. Similarly, the authors of [128, 129, 130] have given solutions to enhance the security of patient's health data which is otherwise prone to misuse.

Some of the most famous blockchain based initiatives that have been taken for managing electronic heath records include the names like Medric [131], Patientory [132], HealthSuite Insights Philips Healthcare, Medshare [133], Iryo, Gem Health, FHIR Chain [134],OMNI PHR [135], Medicalchain, Doc.ai and Hearthy [136].

Similarly, The BC based projects that are focused on genomics include Factom, Encrypgen, Nebula Genomics, lunaDNA, Zenome, Genomes.io and Shivom [136].

ETDB-Caltech [137], Patel et. al 2018, OPU Labs, MedX Protocol, Dermonet [138] are the examples of BC based initiatives in the field of dermatology. The BC based projects initiated in the direction of managing pharmaceutical supply chain solutions like track and trace regulation, track of temperature, humidity, etc. of the pharmaceutical products, and bringing transparency in trade records, include Mediledger project, Ambrosus, Modsense T1, Blockverify, DHL collaboration with Accenture, Authentag, Hejia, GFT collaboration with MYTIGATE, and IEEE pharma supply BC forum [136].

For prescription management, BC initiatives like BlockMedx, Project Heisenberg, ScriptDrop,and ScalaMed [136]. BlockMedx Allows a pharmacist to verify the prescription issue by the doctor by accesing the created immutable BC. Project Heisenberg manages the prescription process by giving different portals to doctors, patients and pharmacists. In ScriptDrop authors have worked to deliver the medicines at the doorsteps of the patients, relieving their burden of visiting the pharmacies once the prescription is issued. ScalaMed offers a patient-centric model for managing this process. ScalaMed keeps a track of all the patient's prescription to avoid cases of cross-reactions of prescribed medicines.

The BC based solutions for billing and claim management include Gem, Change Healthcare, HSBlox, Pokitdox, solve.care, Smartillions, HealthNautica with Factom, and Robomed Network [136].

3.6. Government Services. Gone are the days when criminals would crack safes and loot bank vaults. Today governments all around the world face the wrath of cyber-attacks. Tax frauds happen everywhere which hinder the development of nations. BC has the potential to tackle both of these issues [139]. These along with some other use cases and opportunities provided by BC in the government services are discussed in the

following sub-sections.

Securing important public infrastructure from cyber-attacks. Every nation's critical public infrastructure is implanted with one or the other digital technology and a significant number of the frameworks are also connected through the internet [139]. This opens them to the likelihood of hacking assaults. The countries that have established strong cyber security defenses can also launch the attacks, and go undetected. For example, it is possible to snatch the control of critical routers, monitor, and manipulate them. This would permit the information from any government association behind routers to be caught. Other cyber-attacks to which the e-governments are vulnerable include malware, DDoS, probes, packet sniffing [140]. The motivation for launching these attacks could be to bring political differences, extortion, race for supremacy, and cyber-terrorism [141].

Additionally, as several other digital technologies are incorporated in public infrastructural frameworks like railways, bridges, flood channels, and energy establishments, the possibility that such assaults could cause loss to property and human life increases substantially.

How BC can help: BC's distributed ledger characteristic can make sure that the software and other firmware embedded on the infrastructure has not been meddled with. It can moreover track the state and integrity of the firmware for ensuring integrity and protection of human life.

Financial frauds suffered by the governments. The government departments face issues like [142]:

- Monetary losses because of errors and frauds.
- Problems in efficient policy delivery and complete financial inclusion of poverty-stricken people.
- How to put the public money on a sustainable footing.
- Verifying the true identities of users.
- Problems in the distribution of international aid in the conditions of crisis.

How BC can help: BC can help to tackle these issues in the following manner:

- BC can offer full financial inclusion to people who cannot afford the inclusion barriers like heavy transaction costs, access to customary financial products, etc. BC can include the people easily and in an affordable manner into the benefits system.
- BC will make the forgery of identities extremely difficult and almost impossible [143, 144]. It has the intrinsic building characteristic that it can verify the identities of users through distributed ledgers that run on extremely secure devices. This will slash the level of fraud and errors that are issued in the delivery of benefits.
- The tax-payers can easily check how their money is being invested by the government in the BC-based systems.
- BC's distributed ledgers have no boundaries based on geography, i.e., their modus-operandi remains the same in any part of the world. This feature can offer great relief in removing the bureaucratic hurdles of classical banking systems as the international donors can donate coins. This will not only ease the suffering one faces in sending money overseas but also reduces the international aid exchange fees [145].
- Moreover distributed ledgers can curtail the cash fungibility, i.e., the property of an item whose single units are indistinguishable and have the same value.
- BC solves the problem of double-spending which in the case of international aid reception or tax reception is important to avoid.
- BC's distributed ledger can trace how the currency has been spent and by whom [139]. This assures the aid being spent on purposes other than for which it was provided.

Integrating the resources of a decentralized nation. China, for example is a massively decentralized nation from the perspective of responsibilities and resources given to the local governments [146] which makes the integration of its resources a hurricane task.

How BC can help: Blockchain records every transaction which makes it simple to track the parties that approve transactions and comprehend the extent of the exchange. It additionally implies that information can be all the more effectively and securely moved between various associations, in this manner advancing the incorporation of data among various associations. Moreover, the BC technology primarily relies on a consensus mechanism for its working. This implies that decentralized governments can choose entities that can make additions to a particular BC using a consensus mechanism, thereby developing trust among these entities, and

integrating their resources on one platfor [146].

*Literature survey on current work:*In 2016, the government of United Kingdom affirmed the Fintech startup Credits to be the provider for Blockchain innovation for government organizations, and endorsed the utilization of Block-as-a-Service [147]. The motivation for this adoption was five-fold [148]:

1. for protecting the public infrastructure,
2. It could lead to the development of secure payment frameworks for work and pensions,
3. Reinforcement of international aid systems,
4. document verifications,
5. Managing European VAT system.

Similarly, Dubai government along with some other private entities has established a council called Global Blockchain Council that integrates elements from government, local and international startups to boost the BC technology with various experiments [147]. The authors of [149] have proposed a BC based e-government framework for bringing security and privacy in the operation of various public sectors. Grech et al. illustrate in [150] how BC could be employed in the national identity management systems. However, proper implementation of the proposal has not been given. [151] have described the self-sovereign digital Id system of Canada that is based on BC. However, again no evaluation criteria have been used. [152] suggests the replacement of the bureaucratic government with a BC based government for transparency.

3.7. Tourism. As per the world travel and tourism council's annual report for 185 countries and 25 regions, Tourism industry has contributed a whopping $8.8 trillion to the global economy in the year 2018 [153]. The report published that the industry reckoned for 10.4% of the global economy, 10% of total employment, 6.5% of global exports, and 27.2 % of global service exports. The economic impact of travel and tourism for the year 2019 marked a 3.9% increase over 2018, giving a boost of 2.9% to the total global economy [153]. The Internet has abled the tourists to book their products and other travel related requirements online [142]. From the literature review, it is observed that since the time blockchain caught worldwide consideration in 2017, its potential adoption has progressively changed different ventures. Among these areas, the tourism industry right now leads in blockchain investment [154]. The following sub-sections describe the issues present in the tourism sector and how BC can help to alleviate them.

- Online customer reviews about their travel highly clout the buying choices of tourists. Amateur tourists especially consider the online reviews to be the sincere sentiments of genuine travellers [155]. However, the reliability of these reviews cannot be ascertained completely as there can be the manipulation of centralized systems handling these reviews by hotel and restaurant owners as well as by the customers.
  How BC can help: For having fair reviews, BC can provide a common rating and audit framework that provides reviewers with traceable identities. This, however, does not require giving up the anonymity but that all entries are marked with a private key that is unique to every specific user. Subsequently, tourists would be unable to make duplicate reviews with one identity. Also, nobody will be able to change their reviews ex-post.
- Buying and selling of tourism-related products involve the exchange of money between parties who do not know each other beforehand and money transfers across country borders. To establish trust in these situations, intermediaries are used who charge commissions.
  How BC can help: Bitcoin and other crypto-currencies do not require any third party for money exchange. This empowers the development of new types of client-client exchanges for tourism items.
- Heterogeneous payment gateways are used to pay for availing tourism services. Such gateways in turn open the gates to malicious users for launching attacks like hacking into wallets, theft of identities, attacks on payment clearance cycles, etc. [156].
  How BC can help: Blockchain offers a decentralized architecture for payments that establishes reliance and reputation management among the various parties involved in the tourism industry like, banks, travel agencies, hotel, cabs, etc. [157].
- The market power of Online Travel Agencies (OTAs) and Global Distribution System (GDS) are the intermediaries whose removal is a must from the tourism supply chain [158] for the reason that they encourage the custom of commission and move the market according to their whims, and wishes. The powerful members of the GDS formulate rules and fees that every small tour operator has to comply

with to be competitive.
How BC can help: BC is an open source and decentralized platform which has the potential to do away with these intermediaries. Examples of BC-based online tourism platforms include HotelP2P, and WindingTree [159].

- Small Island Economies (SIEs) are exceptionally reliant on the tourism industry as a critical supporter of their economic development. However, their economic development is encroached by various external financial and ecological factors, their small size and insularity [154]. To beat these inherent difficulties, SIEs need to assemble strength, diversify their economy and create the tourism schemes that encourage economic development [160]. Such an opportunity will be provided by the adoption of blockchain innovation.
  How BC can help: Aruba, a small island economy is building up a blockchain platform to permit local companies to directly associate with tourists, accordingly recovering loss revenues from the monopoly of foreign agencies [154]. While, the Caribbean Tourism Organization is elevating crypto-installment to help the travel industry [154].
- The other tourism related challenges which can be tackled by using the inherent characteristics of BC include the avoidance of overbooking , coordination among hotels and transport systems, assistance in baggage tracking, and verification of travel ID's [156].

Literature survey on current work: [156] proposed a BC based framework called BloHosT (Blockchain Enabled Smart Tourism and Hospitality Management). BloHost uses a single crypto currency enabled application to register the tourists as well as the various tourism stakeholders. For interoperability, it uses smart contracts. Onder and Treiblmaier proposed in 2018 [142] three propositions about blockchain in tourism industry that would bring a completely new look to the tourism industry. Firstly, new forms of evaluations and review technologies will eventually form reliable rating systems; secondly, the extensive adoption of crypto-currencies will pave way to the development of new C2C markets, and finally the BCT will lead to increased disintermediation in the tourism industry. They have argued that answers to these propositions would bring a new look to tourism industry in blockchain perspective. In [161] Leung and Dickinger have dissected how European explorers use Bitcoin as a digital currency to buy tourism products. Besides eliminating the intermediaries, their system offers an uninterrupted service along with the safety of data via immutable encryption. In their work [162], authors have tried to relate the trust in blockchain with the trust in tourism. Pilkington and Crudu [163] have taken a shot at how blockchain can be utilized for diminishing poverty in a poor nation like Moldova with the tourism 2.0. They have contended that because of the high corruption rate in Moldova, there is a requirement for trusted systems. The researchers have exhibited that the immutable nature of blockchain can help mitigate destitution with the tourism 2.0 by wiping out defilement issues in Moldova.

4. Challenges in the way of total realization of Blockchain. To gain a holistic view of the strength of Blockchain technology, it is imperative to discuss the challenges that need to be overcome for its successful implementation in these key areas. This section puts a stress on the limitations of the BC technology.

The first problem area will be the harm to privacy. Bitcoin transactions may be allied to user details which can then be associated to IP addresses, suggesting a lack of anonymity for users. The likelihood of a loss of privacy could undermine the general protection of blockchain infrastructures. Online voting systems, for example, place excessive value on security as a main blockchain property, both to protect voters and to ensure the correctness of the election result. The second problem in the paradigm of voting emerges in the consensus algorithms used in BC with regard to speed and energy consumption. Bitcoin's PoW has an estimated energy intake of 45.8 TWh per annum, according to [164].

The challenges that a company which wishes to adopt Blockchain for improving its food supply chain must overcome relate to the development of smart contracts and endorsement policies, channel configuration and data management. A paper contract consists of different clauses. In order to define constraints for a data model, these contractual clauses can be defined by textual language. These constraints can later be converted into a more formal language. For a smart contract, they can even be translated into code. Once the constraints are in a formal grammar, they can also be tested for consistency, completeness and accuracy using software tools. Blockchain ledger is a database of historical transactions [165]. Mapping a supply chain process into a series of successive transactions that are conducted in an ordered sequence is necessary to incorporate a process on

a blockchain system. While intuitive, there are challenges to operationalizing this approach. The terminology of regulatory policies in plain text, in particular, can be very complicated and such policies are not easy to map into an executable language with the right semantics. The need to ensure that the smart contract code represents the parties' intent and contains no inadvertent coding errors is another major concern. However, ensuring that the software code is bug-free is virtually impossible. Danger is thus not completely removed [166]. This is obviously a weakness of the blockchain technology.

From the viewpoint of IoT security, at present, the Bitcoin block size is limited to 1 MB and a block is mined about every ten minutes. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second. Thus BC is unable to deal with high-frequency trading [167]. The small block capacity means the delay of smaller transactions as the miners would prefer the transactions with higher fees. However, larger block sizes mean larger storage space and slower propagation in the network. This will lead to the branching of blockchain. This makes scalability a huge challenge. The prime feature of IoT is the multitude of devices, hence, overcoming this scalability issue will be a major challenge.

The integration of blockchain into ITS provides data manipulation security and prevention through its ability to guarantee data immutability. Blockchain cannot however, directly guarantee security and privacy, as blockchain is based on various methods. Some of the techniques are modern cryptographic techniques, pseudonyms, and off-chain storage. That can ensure the security of content within blocks (transactions or records) and the privacy of users and devices [168]. Moreover, the incorporation of blockchain in ITS may involve the ability to manage a large number of data and transactions in a highly complex moving vehicle environment. This is a current blockchain application weakness to accommodate into IoV directly [169]. Therefore, the performance metrics of the blockchain enabled IoV network are as critical as its protection and privacy due to the reliance of massive data and mobility. These matrices of performance include latency, consumption of energy, scalability, and throughput. Collusion attacks could be launched in BC-enabled IoV networks because of the issues in consensus algorithms. The active validators may collude with other false validators in this attack [170].

The important challenges that exist in BC-based healthcare systems include scalability, security and privacy of electronic health records because of the 51% attack, heavy processing power requirement, and huge investment by providers to lay down the BC infrastructure in their domains. Keeping the nodes alive in such a BC-based healthcare system across the nation needs enormous socio-technical changes, and alignments [171]. Moreover, BC applications are created to be HIPPA and GDPR compliant. However, as separate social, economic and healthcare structures would be combined, it is problematic for both the patient and the healthcare provider to lack the legal or compliance code to obey the results of the applications [172].

For adopting BC in government services, in addition to the heavy sustainability costs, complicated, expensive, and extensive software upgrades across all the mining computers in the nation is required. Sometimes, due to the existence of a software error, or anomalies in the blocks of a single user that can cause the entire blockchain to break prematurely, protocol changes cannot roll smoothly. All the users in the network will have to rollback their updates in such situations to maintain continuity in the entire blockchain [173]. Next, it is often difficult to introduce deliberate software protocol changes, and seasoned network users must be vigilant and sometimes forcefully avoid such actions. Another big problem that can occur in BC is the loss of cryptographic keys. If any user loses the public/private key package, is stolen or expires, those blocks cannot be recovered [174]. Also, in the long run, BC will display a poor economic behavior because with time the reward that one will get for mining will be less profitable compared to the extensive resource investment [175]. The Proof of work algorithm is highly susceptible to DoS attacks. Critical government infrastructure will be put at risk. Double spending attacks could be launched if one user gets the control of 33% of network computational resources [176].

In the sector of tourism, the usage of blockchain technology by customers would be restricted to those who are tech-savvy and educated about its process, thus limiting its use to just a small demographic group. In addition, in the event of an unexpected shock to the economy, the lack of regulation over blockchain and cryptocurrencies poses a concern for tax evasion and exchange rate volatility. Cryptocurrency value instability may also pose a danger to market stability for potential tourists [177] . Moreover, given the huge energy consumption of blockchain networks, the environmental cost implications for SIEs would require attention to

the production of renewable energy and the related policy reforms [178].

Risk posed by Quantum Computers to Block-chain technology: Block-chain technology uses one-way mathematical functions to generate digital signatures that are required for authenticating the users in the network. These functions are easy to calculate, but very difficult to forge, for the reason that it is extremely hard to calculate the inverse of these functions. However, the advancements in the field of quantum computing are posing a serious threat to the security of block-chains [179]. It is anticipated that in the near future, the quantum computers would be able to calculate the inverse of one-way functions easily, making the encryption using these functions obsolete. Hence, investigating the encryption methods that are hard to break even using quantum computers is highly crucial for the block-chain security.

5. Conclusion and Future Directions. Blockchain is a decentralized, persistent, distributed, immutable, transparent, secure and auditable database technology. Currently, it is viewed as a concept that has tremendous potential to transform the finance industry, but its potential in other areas remains unexplored. In this paper, we examined the integration of BC with seven key scenarios. In each of these scenarios, we highlighted the problems that exist in the classical systems which they use and the solutions that Blockchain technology can provide. We have also highlighted some current issues that require careful analysis and professional research. This research proposes two aspects of the blockchain definition in these sectors at the theoretical level: explicit and implicit. The functional aspects of the blockchain define the explicit dimensions. While most of the scarce research in the field of blockchain is technology-driven, suggesting new protocols and algorithms, attention is not given to the major drawbacks that come with it. This paper in addition to the implicit advantages of using blockchain has highlighted the key challenges that come with its adoption in any of these sectors. It can be used as a guiding torch by the researchers to take up a research challenge in the domain of blockchain. The future directions are given as:

1. *Scalability:* Researchers can shift their focus towards finding a tradeoff between block size and security.
2. *Privacy violation:* According to [180], BC does not assure the transactional privacy maintenance. This is because of the public visibility of all the transaction values and public keys. Moreover, [181] has proved that the Bitcoin transactions carried out by an individual could be served and analyzed to expose the information of a user. Also, a method has been proposed by [182] to attach pseudonyms of users (a key feature of BC) with the IP addresses even in the case when they are secured behind the firewalls or the Network Address Translation (NAT).
   Researchers can go in the direction of finding improvements in the anonymity of BC.
3. *Attacks by miners:* There is a consensus on the statement that if 51% of the computing power of the BC combines, it can reverse the BC and subsequently reverse the successful transactions [167]. Therefore, if the miners become successful in carrying out the collusion attack or otherwise called the 51% attack, the consequences could be heavily dangerous. Moreover, the researchers are vouching on the statement that much less than 51% power is required to cheat in BC [183].
   Other than 51% attacks, stubborn mining [184] where the miners launch network-level eclipse attacks are possible in BC. Researchers can work in the direction of finding approaches to let the honest miners work without just wasting their resources, and in letting them find a BC branch which is neither selfish nor stubborn.
4. *The movement towards centralization:* BC is depicting a trend where miners become centralized in the mining pool. For example, in the Bitcoin network [185], only the top 5 mining pool own more than 51% of the entire hash power.
   Since the BC's strength lies in its decentralized architecture, this trend has to be stopped and for that methods need to be proposed.
5. *Smart contract attack analysis:* Smart contract is a fragment of code that can be automatically executed by the miners. If this code is tampered with, even with a small bug, disastrous damage can happen. An example is the loss of $60 million by the recursive call bug in the DAO- Smart contract.
   Researchers need to focus on the analysis of smart contract attacks.

Acknowledgments. We would like to thank TEQIP-III and MITS, Gwalior for supporting this research.

REFERENCES

[1] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, *A survey on privacy protection in blockchain system*, in Journal of Network and Computer Applications, vol. 126, pp. 45–58, 2019.

[2] G. Fanti and P. Viswanath, *Anonymity properties of the bitcoin p2p network*, arXiv preprint arXiv:1703.08761, 2017.

[3] G. Fanti, S. B. Venkatakrishnan, S. Bakshi, B. Denby, S. Bhargava, A. Miller, and P. Viswanath, *Dandelion++ lightweight cryptocurrency networking with formal anonymity guarantees*, in Proceedings of the ACM on Measurement and Analysis of Computing Systems, vol. 2, no. 2, pp. 1–35, 2018.

[4] L. Yang, V. Bagaria, G. Wang, M. Alizadeh, D. Tse, G. Fanti, and P. Viswanath, *Prism: Scaling bitcoin by 10,000 x*, arXiv preprint arXiv:1909.11261, 2019.

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, *Blockchain in internet of things: challenges and solutions*, arXiv preprint arXiv:1608.05187, 2016.

[6] J. S. Calvery, *Statement of jennifer shasky calvery, director financial crimes enforcement network united states department of the treasury*, Vienna, Virginia, United States: Financial Crimes Enforcement Network, 2013.

[7] *Coin market cap*, accessed 19-02-2019.[Online]. Available: https://coinmarketcap.com/.

[8] *Blockonomi*, accessed 19-02-2019.[Online]. Available: https://blockonomi.com/bitcoinprice/.

[9] S. Huh, S. Cho, and S. Kim, *Managing iot devices using blockchain platform*, in 2017 19th international conference on advanced communication technology (ICACT). IEEE, 2017, pp. 464–467.

[10] M. Conoscenti, A. Vetro, and J. C. De Martin, *Blockchain for the internet of things: A systematic literature review*, in 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). IEEE, 2016, pp. 1–6.

[11] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, *A survey on consensus mechanisms and mining strategy management in blockchain networks*, IEEE Access, vol. 7, pp. 22 328–22 370, 2019.

[12] K. Yeow, A. Gani, R. W. Ahmad, J. J. Rodrigues, and K. Ko, *Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues*, IEEE Access, vol. 6, pp. 1513–1524, 2017.

[13] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, *A survey on the scalability of blockchain systems*, in IEEE Network, vol. 33, no. 5, pp. 166–173, 2019.

[14] C. Decker and R. Wattenhofer, *A fast and scalable payment network with bitcoin duplex micropayment channels*, in Symposium on Self-Stabilizing Systems. Springer, 2015, pp. 3–18.

[15] T. M. Fernandez-Carames and P. Fraga-Lamas, *A review on the use of blockchain for the internet of things*, in IEEE Access, vol. 6, pp. 32 979–33 001, 2018.

[16] A. T. Norman, *Blockchain Technology Explained: The Ultimate Beginners Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA And Smart Contracts* CreateSpace Independent Publishing Platform, 2017.

[17] N. Atzei, M. Bartoletti, and T. Cimoli, *A survey of attacks on ethereum smart contracts (sok)*, in International Conference on Principles of Security and Trust. Springer, 2017, pp. 164–186.

[18] M. Vukolic, *Rethinking permissioned blockchains*, in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM, 2017, pp. 3–7.

[19] C. V. Helliar, L. Crawford, L. Rocca, C. Teodori, and M. Veneziani, *Permissionless and permissioned blockchain diffusion*, in International Journal of Information Management, vol. 54, p. 102136, 2020.

[20] I. Bashir, *Mastering blockchain*, Birmingham: Packt Publishing Ltd, 2017.

[21] S. Haber and W. Stornetta, *How to time-stamp a digital document, crypto'90, lncs 537*, in Springer 1991.

[22] M. Sato and S. Matsuo, *Long-term public blockchain: Resilience against compromise of underlying cryptography*, in 2017 26th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2017, pp. 1–8.

[23] A. Takura, S. Ono, and S. Naito, *A secure and trusted time stamping authority*, in 1999 Internet Workshop. IWS99.(Cat. No. 99EX385). IEEE, 1999, pp. 88–93.

[24] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, *An overview of blockchain technology: Architecture, consensus and future trends,* in 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, 2017, pp. 557–564.

[25] M. Vukolic, *The quest for scalable blockchain fabric: Proof-of-work vs. bft replication*, in International workshop on open problems in network security. Springer, 2015, pp. 112–125.

[26] G. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, and G. Wang, *Compounding of wealth in proof-of-stake cryptocurrencies*, in International Conference on Financial Cryptography and Data Security. Springer, 2019, pp. 42–61.

[27] F. Schuh and D. Larimer, *Bitshares 2.0: General overview*, accessed February-2019.[Online]. Available: https://cryptorating. eu/whitepapers/BitShares/bitshares-general. pdf, 2017.

[28] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, *Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]*, ACM SIGMETRICS Performance Evaluation Review, vol. 42, no. 3, pp. 34–37, 2014.

[29] A. Shoker, *Sustainable blockchain through proof of exercise*, in 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). IEEE, 2017, pp. 1–9.

[30] M. Castro, B. Liskov et al., *Practical byzantine fault tolerance*, in proceeding in OSDI, vol. 99, no. 1999, 1999, pp. 173–186.

[31] D. Schwartz, N. Youngs, A. Britto et al., *The ripple protocol consensus algorithm*, Ripple Labs Inc White Paper, vol. 5, p. 8, 2014.

[32] E. Buchman, *Tendermint: Byzantine fault tolerance in the age of blockchains*, Ph.D. dis- sertation, 2016.

[33] X. Jin and S.-H. G. Chan, *Unstructured peer-to-peer network architectures*, in Handbook of Peer-to-Peer Networking. Springer, 2010, pp. 117–142.

[34] T.T. Kuo, H.-E. Kim, and L. Ohno-Machado, *Blockchain distributed ledger technologies for biomedical and health care applications*, Journal of the American Medical Informatics Association, vol. 24, no. 6, pp. 1211–1220, 2017.
[35] K. M. Khan, J. Arshad, and M. M. Khan, *Investigating performance constraints for blockchain based secure e-voting system*, Future Generation Computer Systems, vol. 105, pp. 13–26, 2020.
[36] M. Pawlak, A. Poniszewska-Maranda, and N. Kryvinska, *Towards the intelligent agents for blockchain e-voting system*, Procedia Computer Science, vol. 141, pp. 239–246, 2018.
[37] B. Sudharsan, N. K. MP, M. Alagappan et al., *Secured electronic voting system using the concepts of blockchain*, in 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2019, pp. 0675–0681.
[38] M. Polasik, A. I. Piotrowska, T. P. Wisniewski, R. Kotkowski, and G. Lightfoot, *Price fluctuations and the use of bitcoin: An empirical inquiry*, in International Journal of Electronic Commerce, vol. 20, no. 1, pp. 9–49, 2015.
[39] A. B. Ayed, *A conceptual secure blockchain-based electronic voting system*, in International Journal of Network Security & Its Applications, vol. 9, no. 3, pp. 01–09, 2017.
[40] R. Hanifatunnisa and B. Rahardjo, *Blockchain based e-voting recording system design*, in 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). IEEE, 2017, pp. 1–6.
[41] F. Hjalmarsson, G. K. Hreiarsson, M. Hamdaqa, and G. Hjalmtysson, *Blockchain-based e-voting system*, in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018, pp. 983–986.
[42] D. D. Kumar, D. Chandini, B. D. Reddy, D. Bhattacharyya, and T.-h. Kim, *Secure electronic voting system using blockchain technology*, International Journal of Advanced Science and Technology, vol. 118, no. 1, pp. 13–22, 2018.
[43] S. Shah, Q. Kanchwala, and H. Mi, *Block chain voting system*, Northeastern University, 2016.
[44] I. Obulesu, A. Hari, and P. Manish, *Prreethi: Iot based fingerprint voting system*, Acad. Sci. Int. J. Innov. Adv. Comput. Sci, vol. 7, no. 4, pp. 502–505, 2018.
[45] Y. Takabatake, D. Kotani, and Y. Okabe, *An anonymous distributed electronic voting system using zerocoin*, in proceedings in Institute of Electronics, Information and Communication Engineers (IEICE), 2016.
[46] F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, *Crypto-voting, a blockchain based e-voting system.* in KMIS, 2018, pp. 221–225.
[47] K. Kirby, A. Masi, and F. Maymi, *Votebook: A proposal for a blockchain-based electronic voting system*, in The Economist, vol. 6, 2016.
[48] R. Osgood, *The future of democracy: Blockchain voting*, in COMP116: Information security, pp. 1–21, 2016.
[49] S. Bistarelli, M. Mantilacci, P. Santancini, and F. Santini, *An end-to-end voting-system based on bitcoin*, in Proceedings of the Symposium on Applied Computing, 2017, pp. 1836–1841.
[50] T. Dimitriou, *Efficient, coercion-free and universally verifiable blockchain-based voting*, in Computer Networks, p. 107234, 2020.
[51] S. Saberi, M. Kouhizadeh, and J. Sarkis, *Blockchains and the supply chain: Findings from a broad study of practitioners*, in IEEE Engineering Management Review, vol. 47, no. 3, pp. 95–103, 2019.
[52] Mattila, Juri and Seppla, Timo and Holmstrom, Jan, *Product-centric information management: A case study of a shared platform with blockchain technology*, in Industry Studies Association Conference, Minneapolis, MN, USA, 2016.
[53] N. Kshetri, *Blockchain's roles in meeting key supply chain management objectives*, in International Journal of Information Management, vol. 39, pp. 80–89, 2018.
[54] P. N. Mahalle, B. Anggorojati, N. R. Prasad, R. Prasad et al., *Identity authentication and capability based access control (iacac) for the internet of things*, Journal of Cyber-Security and Mobility, vol. 1, no. 4, pp. 309–348, 2013.
[55] M. A. Khan and K. Salah, *Iot security: Review, blockchain solutions and open challenges*, in Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.
[56] N. Kshetri, *Blockchain's roles in meeting key supply chain management objectives*, in International Journal of Information Management, vol. 39, pp. 80–89, 2018.
[57] S. Apte and N. Petrovsky, *Will blockchain technology revolutionize excipient supply chain management?*, in Journal of Excipients and Food Chemicals, vol. 7, no. 3, p. 910, 2016.
[58] F. Tian, *An agri-food supply chain traceability system for china based on rfid & blockchain technology*, in 2016 13th international conference on service systems and service management (ICSSSM), IEEE, 2016, pp. 1–6.
[59] T. Moe, *Perspectives on traceability in food manufacture*, Trends in Food Science & Technology, vol. 9, no. 5, pp. 211–214, 1998.
[60] S. Saberi, M. Kouhizadeh, and J. Sarkis, *Blockchains and the supply chain: Findings from a broad study of practitioners*, in IEEE Engineering Management Review, vol. 47, no. 3, pp. 95–103, 2019.
[61] G. Falco, C. Li, P. Fedorov, C. Caldera, R. Arora, and K. Jackson, *Neuromesh: Iot security enabled by a blockchain powered botnet vaccine*, in Proceedings of the International Conference on Omni-Layer Intelligent Systems, 2019, pp. 1–6.
[62] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, *Blockchain's adoption in iot: The challenges and a way forward*, in Journal of Network and Computer Applications, Elsevier, vol. 125, pp. 251–279, 2019.
[63] N. Z. Aitzhan and D. Svetinovic, *Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams*, in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 840–852, 2016.
[64] L. Axon, *Privacy-awareness in blockchain-based PKI*, in Cdt technical paper series, vol. 21, p. 15, 2015.
[65] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, *Blockchain for iot security and privacy: The case study of a smart home*, in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017, pp. 618–623.

[66] T. Hardjono and N. Smith, *Cloud-based commissioning of constrained devices using permissioned blockchains,* in Proceedings of the 2nd ACM international workshop on IoT privacy, trust and security, 2016, pp. 29–36.
[67] *Ibm. hyperledger–ibm blockchain.* accessed 19-02-2020.[Online]. Available: https://www.ibm.com/blockchain/hyperledger.html s-3.
[68] *Projects, t.l.f. hyperledger fabric.* accessed 19-02-2020.[Online]. Available: https://hyperledger.org/projects/fabric.
[69] E. Munsing, J. Mather, and S. Moura, *Blockchains for decentralized optimization of energy resources in microgrid networks*, in 2017 IEEE conference on control technology and applications (CCTA). IEEE, 2017, pp. 2164–2171.
[70] Z. Neha and G. Guerard, *Integration of the blockchain in a smart grid model*, in Proceedings of the 14th International Conference Of Young Scientists On Energy Issues (CYSENI 2017), Kaunas, Lithuania, 2017, pp. 25–26.
[71] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, *Towards a novel privacy-preserving access control model based on blockchain technology in iot*, in Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, 2017, pp. 523–533.
[72] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, *Towards blockchain-based auditable storage and sharing of iot data*, in Proceedings of the 2017 on Cloud Computing Security Workshop, 2017, pp. 45–50.
[73] M. Vucinic, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, *Oscar: Object security architecture for the internet of things*, in Ad Hoc Networks, vol. 32, pp. 3–16, 2015.
[74] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, *Privacy-preserving andvefficient aggregation based on blockchain for power grid communications in smart communities*, in IEEE Communications Magazine, vol. 56, no. 7, pp. 82–88, 2018.
[75] M. Mettler, *Blockchain technology in healthcare: The revolution starts here*, in 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom). IEEE, 2016, pp. 1–3.
[76] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, *LSB: A lightweight scalable blockchain for iot security and anonymity*, in Journal of Parallel and Distributed Computing, vol. 134, pp. 180–197, 2019.
[77] P. Ghuli, U. P. Kumar, and R. Shettar, *A review on blockchain application for decentralized decision of ownership of iot devices*, Adv. Comput. Sci. Technol, vol. 10, no. 8, pp. 2449–2456, 2017.
[78] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, *World of empowered iot users*, in 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, 2016, pp. 13–24.
[79] S. Huh, S. Cho, and S. Kim, *Managing iot devices using blockchain platform*, in 2017 19th international conference on advanced communication technology (ICACT). IEEE, 2017, pp. 464–467.
[80] B. Leiding, C. H. Cap, T. Mundt, and S. Rashidibajgan, *Authcoin: validation and authentication in decentralized networks*, arXiv preprint arXiv:1609.04955, 2016.
[81] L. Wu, X. Du, W. Wang, and B. Lin, *An out-of-band authentication scheme for internet of things using blockchain technology,* in 2018 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2018, pp. 769–773.
[82] M. English, S. Auer, and J. Domingue, *Block chain technologies & the semantic web: A framework for symbiotic development,* in Computer Science Conference for University of Bonn Students, J. Lehmann, H. Thakkar, L. Halilaj and R. Asmat, Eds. sn, 2016, pp. 47–61.
[83] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, *Iot passport: a blockchain-based trust framework for collaborative internet-of-things,* in Proceedings of the 24th ACM Symposium on Access Control Models and Technologies, 2019, pp. 83–92.
[84] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, *A blockchain connected gateway for ble-based devices in the internet of things,* in IEEE Access, vol. 6, pp. 24 639–24 649, 2018.
[85] J. Herbert and A. Litchfield, *A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology*, in Proceedings of the 38th Australasian computer science conference (ACSC 2015), vol. 27, 2015, p. 30.
[86] Y. Zhang and J. Wen, *An iot electric business model based on the protocol of bitcoin*, in 2015 18th international conference on intelligence in next generation networks. IEEE, 2015, pp. 184–191.
[87] A. Bahga and V. K. Madisetti, *Blockchain platform for industrial internet of things*, in Journal of Software Engineering and Applications, vol. 9, no. 10, pp. 533–546, 2016.
[88] W. Xu, W. Trappe, Y. Zhang, and T. Wood, *The feasibility of launching and detecting jamming attacks in wireless networks*, in Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. ACM, 2005, pp. 46–57.
[89] G. Noubir and G. Lin, *Low-power dos attacks in data wireless lans and countermeasures*, ACM SIGMOBILE Mobile Computing and Communications Review, vol. 7, no. 3, pp. 29–30, 2003.
[90] S. H. Chae, W. Choi, J. H. Lee, and T. Q. Quek, *Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone*, in IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1617–1628, 2014.
[91] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Enhancing physical-layer secrecy in multi-antenna wireless systems: An overview of signal processing approaches,* in IEEE Signal Processing Magazine, vol. 30, no. 5, pp. 29–40, 2013.
[92] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, *Channel-based detection of sybil attacks in wireless networks*, in IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 492–503, 2009.
[93] Y. Chen, W. Trappe, and R. P. Martin, *Detecting and localizing wireless spoofing attacks*, in 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. IEEE, 2007, pp. 193–202.
[94] S. Shiaeles, N. Kolokotronis, and E. Bellini, *IoT vulnerability data crawling and analysis*, in 2019 IEEE World Congress on Services (SERVICES), vol. 2642. IEEE, 2019, pp. 78–83.

[95] T. Bhattasali and R. Chaki, *A survey of recent intrusion detection systems for wireless sensor network*, in International conference on network security and applications. Springer, 2011, pp. 268–280.
[96] H. Kim, *Protection against packet fragmentation attacks at 6lowpan adaptation layer*, in 2008 International Conference on Convergence and Hybrid Information Technology. IEEE, 2008, pp. 796–801.
[97] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, *6lowpan fragmentation attacks and mitigation mechanisms*, in Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks. ACM, 2013, pp. 55–66.
[98] K. Weekly and K. Pister, *Evaluating sinkhole defense techniques in rpl networks*, in 2012 20th IEEE International Conference on Network Protocols (ICNP). IEEE, 2012, pp. 1-6.
[99] F. Ahmed and Y.-B. Ko, *Mitigation of black hole attacks in routing protocol for low power and lossy networks*, in Security and Communication Networks, vol. 9, no. 18, pp. 5143–5154, 2016.
[100] M. Brachmann, O. Garcia-Morchon, and M. Kirsche, *Security for practical coap applications: Issues and solution approaches*, GI/ITG KuVS Fachgesprch Sensornetze (FGSN). Universitt Stuttgart, 2011.
[101] J. Granjal, E. Monteiro, and J. S. Silva, *End-to-end transport-layer security for internet-integrated sensing applications with mutual and delegated ecc public-key authentication,* in 2013 IFIP Networking Conference. IEEE, 2013, pp. 1–9.
[102] N. Park and N. Kang, *Mutual authentication scheme in secure internet of things technology for comfortable lifestyle*, Sensors, vol. 16, no. 1, p. 20, 2016.
[103] M. H. Ibrahim, *Octopus: An edge-fog mutual authentication scheme*, in IJ Network Security, vol. 18, no. 6, pp. 1089–1101, 2016.
[104] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, *End-to-end transport security in the ip-based internet of things*, in 2012 21st International Conference on Computer Communications and Networks (ICCCN). IEEE, 2012, pp. 1–5.
[105] J. Granjal, E. Monteiro, and J. S. Silva, *Application-layer security for the wot: Extending coap to support end-to-end message security for internet-integrated sensing applications*, in International Conference on Wired/Wireless Internet Communication. Springer, 2013, pp. 140–153.
[106] S. Huh, S. Cho, and S. Kim, *Managing iot devices using blockchain platform*, in 2017 19th international conference on advanced communication technology (ICACT). IEEE, 2017, pp. 464–467.
[107] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, *Blockchain: A distributed solution to automotive security and privacy*, in IEEE Communications Magazine, vol. 55, no. 12, pp. 119–125, 2017.
[108] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, 2014.
[109] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, *Dynamic groups and attribute-based access control for next-generation smart cars*, in Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, 2019, pp. 61–72.
[110] M. Charlie and C. Valasek, *Remote exploitation of an unaltered passenger vehicle*, Black Hat USA, vol. 2015, p. 91, 2015.
[111] Y. Zhe, K. Z. Kan Yang, Lei Lei, and V. C. Leung, *Blockchain-based decentralized trust management in vehicular networks*, in IEEE Internet of Things, vol. 6, no. 2, pp. 1495–1505, 2018.
[112] S. Madhusudan and S. Kim, *Branch based blockchain technology in intelligent vehicle,* in Computer Networks, vol. 145, pp. 219–231, 2018.
[113] L. Ao, Y. C. Haitham Cruickshank, C. P. A. O. Philip Asuquo, and Z. Sun, *Blockchain-based dynamic key management for heterogeneous intelligent transportation systems*, in IEEE Internet of Things, vol. 4, no. 6, pp. 1832–1843, 2017.
[114] L. Lun, L. C. Jiqiang Liu, X. Z. Shuo Qiu, Wei Wang, and Z. Zhang, *Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles*, in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2204–2220, 2018.
[115] R. Qilei, B. G. Ka Lok Man, Muqing Li, and J. Ma, *Intelligent design and implementation of blockchain and internet of things-based traffic system*, Distributed Sensor Networks, vol. 15, no. 8, 2019.
[116] C. Mumin, H. A. Enes Erdin, Kemal Akkaya, and S. Uluagac, *Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles*, in IEEE Communications Magazine, vol. 56, no. 10, pp. 50–57, 2018.
[117] C. Rajat, G. S. A. Anish Jindal, N. K. Shubhani Aggarwal, and K.-K. R. Choo, *Best: Blockchain-based secure energy trading in sdn-enabled intelligent transportation system*, in Computers and Security, vol. 85, pp. 288–299, 2019.
[118] M. Vukolic, *The quest for scalable blockchain fabric: Proof-of-work vs. bft replication*, in International workshop on open problems in network security. Springer, 2015, pp. 112–125.
[119] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, *Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control*, in Journal of medical systems, vol. 40, no. 10, p. 218, 2016.
[120] J.-T. Lorenz, B. Munstermann, M. Higginson, P. B. Olesen, N. Bohlken, and V. Ricciardi, *Blockchain in insurance-opportunity or threat*,in McKinsey & Company Insurance, no. 6, 2016.
[121] D. Blough, M. Ahamad, L. Liu, and P. Chopra, *Medvault: Ensuring security and privacy for electronic medical records*, in NSF CyberTrust Principal Investigators Meeting. Online at http://www. cs. yale. edu/cybertrust08/posters/posters/158 medvault poster CT08.pdf, 2008.
[122] O. Elkeelany, M. M. Matalgah, K. P. Sheikh, M. Thaker, G. Chaudhry, D. Medhi, and J. Qaddour, *Performance analysis of ipsec protocol: encryption and authentication*, in 2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333), vol. 2. IEEE, 2002, pp. 1164–1168.
[123] K. Lauter, *The advantages of elliptic curve cryptography for wireless security*, in IEEE Wireless communications, vol. 11,

no. 1, pp. 62–67, 2004.
[124] G. F. Anderson and B. K. Frogner, *Health spending in OECD countries: obtaining value per dollar*, in Health Affairs, vol. 27, no. 6, pp. 1718–1727, 2008.
[125] E. R and N. SB, *Fundamentals of Database Systems*, Boston, Massachusetts, United States: Pearson Education, 2016.
[126] S. Kabinna, C.-P. Bezemer, W. Shang, and A. E. Hassan, *Logging library migrations: a case study for the apache software foundation projects*, in 2016 IEEE/ACM 13th Working Conference on Mining Software Repositories (MSR). IEEE, 2016, pp. 154–164.
[127] S. Tanwar, K. Parekh, and R. Evans, *Blockchain-based electronic healthcare record system for healthcare 4.0 applications*, in Journal of Information Security and Applications, vol. 50, p. 102407, 2020.
[128] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, *Integrating blockchain for data sharing and collaboration in mobile healthcare applications*, in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2017, pp. 1–5.
[129] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, *Blochie: a blockchain-based platform for healthcare information exchange*, in 2018 ieee international conference on smart computing (smartcomp). IEEE, 2018, pp. 49–56.
[130] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, *Blockchain-based data preservation system for medical data*, in Journal of medical systems, vol. 42, no. 8, p. 141, 2018.
[131] A. Ekblaw and A. Azaria, *Medrec: Medical data management on the blockchain*, in Viral Communications, 2016.
[132] C. McFarlane, M. Beer, J. Brown, and N. Prendergast, *Patientory: A healthcare peer-to-peer emr storage network v1*, Entrust Inc.: Addison, TX, USA, 2017.
[133] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, *Medshare: Trust-less medical data sharing among cloud service providers via blockchain*, in IEEE Access, vol. 5, pp. 14 757–14 767, 2017.
[134] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, *Fhirchain: applying blockchain to securely and scalably share clinical data*, Computational and structural biotechnology journal, vol. 16, pp. 267–278, 2018.
[135] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, *Omniphr: A distributed architecture model to integrate personal health records*, in Journal of biomedical informatics, vol. 71, pp. 70–81, 2017.
[136] G. J. Katuwal, S. Pandey, M. Hennessey, and B. Lamichhane, *Applications of blockchain in healthcare: current landscape & challenges*, arXiv preprint arXiv:1812.02776, 2018.
[137] D. R. Ortega, C. M. Oikonomou, H. J. Ding, P. Rees-Lee, Alexandria, and G. J. Jensen, *Etdb-caltech: a blockchain-based distributed public database for electron tomography*, PloS one, vol. 14, no. 4, p. e0215531, 2019.
[138] V. Patel, *A framework for secure and decentralized sharing of medical imaging data via blockchain consensus*, Health informatics journal, vol. 25, no. 4, pp. 1398–1411, 2019.
[139] M. Walport et al., *Distributed ledger technology: Beyond blockchain*, UK Government Office for Science, vol. 1, 2016.
[140] C. Birkinshaw, E. Rouka, and V. G. Vassilakis, *Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks*, in Journal of Network and Computer Applications, vol. 136, pp. 71–85, 2019.
[141] L. Pau, *Business and social evaluation of denial of service attacks of communications networks in view of scaling economic counter-measures*, in 2010 IEEE/IFIP Network Operations and Management Symposium Workshops. IEEE, 2010, pp. 126–133.¨
[142] I. Onder, H. Treiblmaier et al., *Blockchain and tourism: Three research propositions*, Annals of Tourism Research, vol. 72, no. C, pp. 180–182, 2018.
[143] J. Mattila, *The blockchain phenomenon–the disruptive potential of distributed consensus architectures*, ETLA working papers, Tech. Rep., 2016.
[144] D. Shrier, W. Wu, and A. Pentland, *Blockchain & infrastructure (identity, data security)*, Massachusetts Institute of Technology-Connection Science, vol. 1, no. 3, pp. 1–19, 2016.
[145] S. Ammous, *Economics beyond financial intermediation: Digital currencies potential for growth, poverty alleviation and international development*, in Journal of Private Enterprise, vol. 30, no. 3, pp. 19–50, 2015.
[146] H. Hou, *The application of blockchain technology in e-government in china*, in 2017 26th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2017, pp. 1–4.
[147] A. Alketbi, Q. Nasir, and M. A. Talib, *Blockchain for government services–use cases, security benefits and challenges*, in 2018 15th Learning and Technology Conference (L&T). IEEE, 2018, pp. 112–119.
[148] S. Olnes and A. Jansen, *Blockchain technology as s support infrastructure in e-government*, in International Conference on Electronic Government. Springer, 2017, pp. 215–227.
[149] N. Elisa, L. Yang, F. Chao, and Y. Cao, *A framework of blockchain-based secure and privacy-preserving e-government system*, Wireless Networks, pp. 1–11, 2018.
[150] A. Grech and A. F. Camilleri, *Blockchain in education*, Luxembourg: Publications Office of the European Union 2017, 132 S. - (JRC Science for Policy Report) - URN: urn:nbn:de:0111-pedocs-150132, 2017.
[151] M. Pisa and M. Juden, *Blockchain and economic development: Hype vs. reality*, Center for Global Development Policy Paper, vol. 107, p. 150, 2017.
[152] M. Jun, *Blockchain government-a next form of infrastructure for the twenty-first century*,in Journal of Open Innovation: Technology, Market, and Complexity, vol. 4, no. 1, p. 7, 2018.
[153] A. I. Ozdemir, I. M. Ar, and I. Erol, *Assessment of blockchain applications in travel and tourism industry*, in Quality & Quantity, pp. 1–15, 2019.
[154] A. O. Kwok and S. G. Koh, *Is blockchain technology a watershed for tourism development?*, Current Issues in Tourism, vol. 22, no. 20, pp. 2447–2452, 2019.
[155] R. Filieri, *What makes an online consumer review trustworthy?*, Annals of Tourism Research, vol. 58, pp. 46–64, 2016.

[156] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, and M. Obaidat, *Blohost: Blockchain enabled smart tourism and hospitality management*, in 2019 International Conference on Computer, Information and Telecommunication Systems (CITS). IEEE, 2019, pp. 1–5.
[157] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, *Privacy-preserving energy trading using consortium blockchain in smart grid*,in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3548–3558, 2019.
[158] E. Colombo and R. Baggio, *Tourism distribution channels: Knowledge requirements*, in Knowledge transfer to and within tourism: Academic, industry and government bridges. Emerald Publishing Limited, 2017, pp. 289–301.
[159] R. C. Ford, Y. Wang, and A. Vestal, *Power asymmetries in tourism distribution networks*,in Annals of Tourism Research, vol. 39, no. 2, pp. 755–779, 2012.
[160] L. Dwyer, *Computable general equilibrium modelling: an important tool for tourism policy analysis*, in Tourism and Hospitality Management, vol. 21, no. 2, pp. 111–126, 2015.
[161] D. Leung and A. Dickinger, *Use of bitcoin in online travel product shopping: The european perspective*, in Information and communication technologies in tourism 2017. Springer, 2017, pp. 741–754.
[162] D. Calvaresi, M. Leis, A. Dubovitskaya, R. Schegg, and M. Schumacher, " *Trust in tourism via blockchain technology: results from a systematic review*, in Information and communication technologies in tourism 2019. Springer, 2019, pp. 304–317.
[163] M. Pilkington, R. Crudu, and L. G. Grant, *Blockchain and bitcoin as a way to lift a country out of poverty-tourism 2.0 and e-governance in the republic of moldova*, in International Journal of Internet Technology and Secured Transactions, vol. 7, no. 2, pp. 115–143, 2017.
[164] C. Stoll, L. KlaaBen, and U. Gallersdorfer, *The carbon footprint of bitcoin*, Joule, vol. 3, no. 7, pp. 1647–1661, 2019.
[165] A. Kumar, R. Liu, and Z. Shan, *Is blockchain a silver bullet for supply chain management? technical challenges and research opportunities*, in Decision Sciences, vol. 51, no. 1, pp. 8–37, 2020.
[166] E. Mik, *Smart contracts: terminology, technical limitations and real world complexity*, Law, Innovation and Technology, vol. 9, no. 2, pp. 269–300, 2017.
[167] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, *Blockchain challenges and opportunities: A survey*, in International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.
[168] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, *Blockchain for the internet of vehicles towards intelligent transportation systems: A survey*, in IEEE Internet of Things Journal, 2020.
[169] B. Chen, L. Wu, H. Wang, L. Zhou, and D. He, *A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks*, in IEEE Transactions on Vehicular Technology, 2019.
[170] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, *Blockchain enabled trust-based location privacy protection scheme in vanet*, in IEEE Transactions on Vehicular Technology, vol. 69, no. 2, pp. 2034–2048, 2019.
[171] A. P. Joshi, M. Han, and Y. Wang, *A survey on security and privacy issues of blockchain technology*, in Mathematical foundations of computing, vol. 1, no. 2, p. 121, 2018.
[172] E. Karafiloski and A. Mishev, *Blockchain solutions for big data challenges: A literature review*, in IEEE EUROCON 2017-17th International Conference on Smart Technologies. IEEE, 2017, pp. 763–768.
[173] B. Biswas and R. Gupta, *Analysis of barriers to implement blockchain in industry and service sectors*, in Computers & Industrial Engineering, vol. 136, pp. 225–241, 2019.
[174] S. Seebacher and M. Maleshkova, *A model-driven approach for the description of blockchain business networks*, in Proceedings of the 51st Hawaii International Conference on System Sciences, 2018.
[175] R. Bohme, N. Christin, B. Edelman, and T. Moore, *Bitcoin: Economics, technology, and governance*, Journal of economic Perspectives, vol. 29, no. 2, pp. 213–38, 2015.
[176] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, *Optimal selfish mining strategies in bitcoin*, in International Conference on Financial Cryptography and Data Security. Springer, 2016, pp. 515–532.
[177] M. Polasik, A. I. Piotrowska, T. P. Wisniewski, R. Kotkowski, and G. Lightfoot, *Price fluctuations and the use of bitcoin: An empirical inquiry*, in International Journal of Electronic Commerce, vol. 20, no. 1, pp. 9–49, 2015.
[178] M. Dornan and K. U. Shah, *Energy policy, aid, and the development of renewable energy resources in small island developing states*, in Energy Policy, vol. 98, pp. 759–767, 2016.
[179] K. Dasgupta and M. R. Babu , *A review on crypto-currency transactions using IOTA (technology)*, in Social Network Forensics, Cyber Security, and Machine Learning. Springer, 2019, pp. 67–81.
[180] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, *A fistful of bitcoins: characterizing payments among men with no names*, in Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013, pp. 127–140.
[181] J. Barcelo, *User privacy in the public bitcoin blockchain*, URL: http://www. dtic. upf. edu/˜ jbarcelo/papers/20140704 User Privacy in the Public Bitcoin Blockc hain/paper.pdf (Accessed 09/05/2019), 2014.
[182] A. Biryukov, D. Khovratovich, and I. Pustogarov, *Deanonymisation of clients in bitcoin p2p network*, in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014, pp. 15–29.
[183] I. Eyal and E. G. Sirer, *Majority is not enough: Bitcoin mining is vulnerable*, in Communications of the ACM, vol. 61, no. 7, pp. 95–102, 2018.
[184] K. Nayak, S. Kumar, A. Miller, and E. Shi, *Stubborn mining: Generalizing selfish mining and combining with an eclipse attack*, in 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016, pp. 305–320.
[185] K. Dowd and M. Hutchinson, *Bitcoin will bite the dust*, in Cato J., vol. 35, p. 357, 2015.

Edited by: Dana Petcu
Received: Feb 10, 2021
Accepted: Sep 30, 2021