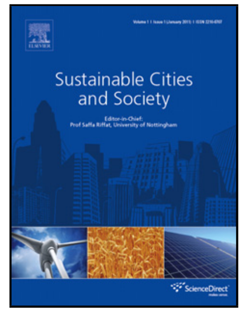
Journal Pre-proof



Blockchain for Smart Cities: A review of Architectures, Integration Trends and Future Research Directions

Bharat Bhushan, Aditya Khamparia, K. Martin Sagayam, Sudhir Kumar Sharma, Mohd Abdul Ahad, Narayan C. Debnath

PII: S2210-6707(20)30581-3

DOI: https://doi.org/10.1016/j.scs.2020.102360

Reference: SCS 102360

To appear in: *Sustainable Cities and Society*

Received Date: 28 March 2020

Revised Date: 27 June 2020

Accepted Date: 27 June 2020

Please cite this article as: Bhushan B, Khamparia A, Martin Sagayam K, Sharma SK, Ahad MA, Debnath NC, Blockchain for Smart Cities: A review of Architectures, Integration Trends and Future Research Directions, *Sustainable Cities and Society* (2020), doi: https://doi.org/10.1016/j.scs.2020.102360

Blockchain for Smart Cities: A review of Architectures, Integration Trends and Future Research Directions

Bharat Bhushan[1#]
Dept. of computer science and engineering, Birla Institute of Technology, Mesra, Jharkhand, 835215, India[1#]
+91-9654879365[1#]
bharat_bhushan1989@yahoo.com[1#]
Postal Address: 282, Metro Apartments, Jahangir Puri, New Delhi, 110033, India[1#]
[#]Corresponding Author[1#]

Aditya Khamparia[2]
School of Computer Science and Engineering, Lovely Professional University, Punjab, 144411, India[2]
aditya.khamparia88@gmail.com[2]

K. Martin Sagayam[3]
Department of Electronics and Communication Engineering[3]
Karunya Institute of Technology and Sciences, Coimbatore, Tamil nade-641114, India[3]
martinsagayam.k@gmail.com[3]

Sudhir Kumar Sharma[4]
Institute of Information Technology and Management, Janakpuri, New Delhi, 110058, India[4]
sharmasudhir08@gmail.com[4]

Mohd Abdul Ahad[5]
Department of Computer Science and Engineering,
School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, 110062, India.[5]
itsmeahad@gmail.com[5]

Narayan C. Debnath[6]
School of Computing and Information Technology, Eastern International University, Vietnam.[6]
NdebnathC@gmail.com[6]

Highlights:

- Presents the state-of-the-art blockchain technology to solve the security issues of smart cities.
- Describes characteristics, security requirements, issues and challenges of smart cities.

- Presents the motivation behind applying blockchain technology to smart cities.
- Highlights the utility of blockchain in various smart communities.

Abstract:

In recent years, smart city has emerged as a new paradigm to provide high quality facilities to the citizens by dynamically optimising the city resources. Smart cities can offer finest services for boosting the daily life of citizens on healthcare, transportation, energy consumption, and education. However, the concept of smart city is still evolving and despite its potential vision, there are proliferating security challenges. Blockchain has the potential to promote the development of smart cities owing to its good properties such as auditability, transparency, immutability and decentralization. Therefore, this paper presents the state-of-the-art blockchain technology to solve the security issues of smart cities. Initially, the paper throws light on the background knowledge and then surveys the utility of blockchain in various smart communities such as healthcare, transportation, smart grid, supply chain management, financial systems and data center networks. Finally, some future research directions are identified through extensive literature survey on blockchain based smart city systems.

Keywords: Smart cities, Blockchain, Security, Privacy, Consensus Protocols, Smart Contract, Smart Communities.

1. Introduction

The past few decades have witnessed a meteoric rise in the world's population that lived in urban area. Nowadays, more than 55 % of the world population are living in urban areas and over the next 30 years, this rate is predicted to reach 70 %, as by 2050, an additional 25 billion people are predicted to move to urban areas [1, 2]. The explosive growth in the world's population coupled with the rapid urbanisation process brings forth numerous social, technical, organizational and economic problems, which tend to endanger the environmental and economical sustainability of cities. Hence, majority of governments are actively interested in adopting "smart" concepts to optimize the use of both tangible (e.g., natural resources, energy distribution networks, and transport infrastructures) and intangible assets (e.g., organizational capital in public administration systems, intellectual capital of companies and human capital) [3, 4]. In this regard, the concept of "Smart City" is proposed that use modern Information and Communication technology (ICT) in an intelligent manner aimed to build a sustainable urban environment and improve the QoL. The smart city has huge range of applications in the modern societies such as smart building for managing the temperature and lighting system [5]; smart energy for optimizing energy consumption using digital technologies; smart healthcare to promote diagnostics [6 – 8]; smart technology to enable edge processing and intelligent network connectivity [9]; smart education to facilitate the education system using modern technologies; smart governance to provide digital services and policies from the government [10]; smart security to reduce security risks and protect properties, people and information [11].

In contrast to the traditional methods, blockchain technology (that was originally designed for Bitcoin cryptocurrency) facilitate transfer of digital assets among peers without any intermediaries [12, 13]. Since, its inception by Santoshi Nakamoto in 2009, Bitcoin witnessed tremendous growth with the capital market [14]. Blockchain is a decentralized, publicly available and immutable shared database that revolutionized the way peers automate payments, interact, trace and track transactions by completely eliminating the need of a central authority for governing the transactions. In traditional systems, the collected data by smart city devices are stored on a central server for future use. These central servers are susceptible to several challenges such as revealing of sensitive information due to hacking of unencrypted server data and the need for more than one management authority at a time [15]. This brings forth the need for a paradigm shift towards a decentralized architecture for storage and management of data [16]. In this context, blockchain enables two devices to communicate and exchange data, information and resources in a decentralized Peer-to-Peer (P2P) network. Further, the blockchain based systems incur minimized overall security monitoring cost and provides security against adversaries trying to gain access to personal information or control over the entire system.

Owing to the widespread adoption of blockchain technology, there have been a number of previously published surveys, such as those presented in **Table 1**. For example, Tschorsch et al. [17] described bitcoin, their building blocks and core of the bitcoin protocol. Christidis et al. [18] described how a blockchain based

IoT systems facilitates resource sharing in a verifiable manner. Similarly, Yeow et al. [19] highlighted various security issues related to edge centric distributed IoT systems and outlined the security challenges therein. In another work, Kouicem et al. [20] focussed on various security requirements for IoT applications and integration of Software Defined Networking (SDN) and blockchain technology. Similarly, Reyna et al. [21] analysed unique features of blockchain technology and outlined various ways of integrating IoT and blockchain. Salman et al. [22] focussed on the use of blockchain technology to ensure secure network services and outlined associated challenges with the proposed blockchain based approaches. In another work, Xie at al. [23] surveyed the state-of-the art blockchain technology that improves the security, efficiency, smartness and performance of smart cities. Similarly, Ferrag et al. [24] surveyed existing blockchain protocols for IoT networks and provided a classification of threat models. Syed et al. [25] presented fundamental concepts of core blockchain architecture and its application in three major area: vehicular industry, healthcare business and IoT. In another study, Sookhak et al. [26] outlined the privacy issues in smart cities. Similarly, Aggarwal et al. [27] surveyed the use of blockchain technology for smart communities and studied various process models related to secure execution of transactions. Sengupta et al. [28] reviewed various attacks in an IoT system and highlighted the benefits of integrating blockchain with various IoT and Industrial IoT applications. Moniruzzaman et al. [29] reviewed current advancements of employing blockchain in smart homes and presented two case studies in this regard. Khan et al. [30] studied blockchain technology and presented its current state-of-the-art in non-financial applications such as healthcare.

Table 1: A comparative summary of existing related surveys

Reference	**Publication Year**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Tschorsch et al. [17]	2016	Y	Y	-	-	-	-	-	-	-	Y	-
Christidis et al. [18]	2016	Y	Y	-	Y	-	-	-	-	-	-	-
Yeow et al. [19]	2017	Y	Y	-	-	-	-	-	-	-	-	Y
Kouicem et al. [20]	2018	-	-	Y	Y	-	Y	Y	Y	-	-	-
Reyna et al. [21]	2018	Y	Y	-	Y	-	-	-	-	-	-	-
Salman et al. [22]	2019	Y	Y	-	Y	-	-	-	-	Y	Y	-
Xie at al. [23]	2019	Y	-	Y	-	Y	Y	Y	Y	Y	-	-
Ferrag et al. [24]	2019	Y	Y	-	Y	-	Y	Y	-	-	-	-

Syed et al. [25]	2019	Y	Y	-	Y	-	Y	Y	-	-	Y	-
Sookhak et al. [26]	2019		-	Y	Y	-	-	-	-	-	-	Y
Aggarwal et al. [27]	2019	Y	Y	-	-	Y	Y	Y	Y	-	Y	Y
Sengupta et al. [28]	2020	Y	-	-	Y	-	Y	Y	Y	Y	-	-
Moniruzzaman et al. [29]	2020	Y	-	-	Y	Y	-	-	Y	-	Y	-
Khan et al. [30]	2020	Y	Y	-	Y	-	Y	-	Y	-	-	-

1: Blockchain basics; 2: Consensus Protocols; 3: Characteristics and Pillars of Smart City; 4: Security requirements and challenges; 5: Blockchain for Smart Cities; 6: Smart Healthcare; 7: Smart Transportation; 8: Smart Grid; 9: Supply Chain Management; 10: Financial Systems; 11: Data Center Networks.

Although blockchain technology and smart cities have been extensively studied in numerous published literature surveys, these two important areas have been researched separately in majority of these existing studies. Moreover, to the best of our knowledge, there is no past surveys that profoundly addresses the role of blockchain in realising security and privacy in smart cities despite its potential. To fill this gap, this paper presents the state-of-the-art blockchain technology to solve the security issues of smart cities. In summary, the key contributions of this article are as follows.

- This work presents state-of-the-art blockchain technology including blockchain architecture, consensus protocols, applications, trade-off and challenges.
- This work focusses more over research on adopting blockchain technology to improve the efficiency, security and performance of smart cities.
- This work surveys the utility of blockchain in various smart communities such as healthcare, transportation, smart grid, supply chain management, financial systems and data center networks.
- This work reviews the existing security requirements, issues and challenges of smart cities aimed to identify the open challenges that can be used as future research directions.

The remainder of the paper is organized as follows: Section 2 presents the background and architecture of blockchain technology. Section 3 describes various features of a smart city. Section 4 throws light on motivations behind applying blockchain technology to smart cities. Section 5 explores existing blockchain efforts in various aspects of smart cities. Finally, future research directions are identified in Section 6 followed by conclusion in Section 7.

2. Blockchain: Background and Architecture

In general terms, blockchain is a continuously growing chain of blocks capable of storing all the committed transactions with the help of a public ledger where every transaction is cryptographically verified and signed by all mining nodes. The following section presents the block structure, types, consensus protocols and the basic architecture of blockchain.

2.1 Block Structure

Similar to a public ledger, blockchain is a sequence of blocks that store information related to all transactions and are linked together via reference hash belonging to the previous block (hash block). The starting block or the parent block is called the genesis block. Generally, a block consists of a block body (that includes transactions and the transaction counter) along with a header (that includes metadata such as nonce, nBits, timestamp, Merkle tree root hash, parent block hash and the block version) [31 – 33]. The attributes of a block header are presented in **Table 2**.

Table 2 Attributes of a block header

SI. No.	Header attributes	Description
1.	Nonce	A 4-byte field that starts from zero and increments for every hash function.
2.	nBits	Compact representation of the current hashing target.
3.	Timestamps	Current timestamp.
4.	Merkle root tree	The calculated hash of all the transactions
5.	Previous block	A 256-bit hash pointing towards the previous block.
6.	Block version	Used to finalize the block validation rule to be followed.

In general, a transaction is a data structure that exemplify transfer of digital assets among peers in a blockchain network and are propagated in the network with the help of gossip protocol, a flooding-based scheme. A transaction is included in a block after it is successfully verified and validated by the miners (peers who mine the blocks on the cost of its computational power) [34, 35]. The miner nodes spend significant amount of computing resources owing to the complex computational puzzle that the miners need to solve. The miner who solves the puzzle first is declared the winner and gets the opportunity to create a new block for which it receives some incentive. Further, all other peers use consensus mechanism (technique using which participants in a decentralized network agrees on a certain matter) to verify the new block. After this, the new block is appended to the existing chain and the next blocks are associated with the newly created block with the help of a cryptographic hash pointer [36 – 38]. In order to validate the transaction's authenticity, blockchain employs asymmetric cryptography mechanism such as digital signatures. Every network participant owns a pair of public and private key. The public key is visible to everyone, distributed throughout the network and used to decryption while the private key is used for encrypting or signing the transaction. The general blockchain architecture is shown in **Figure 1.**

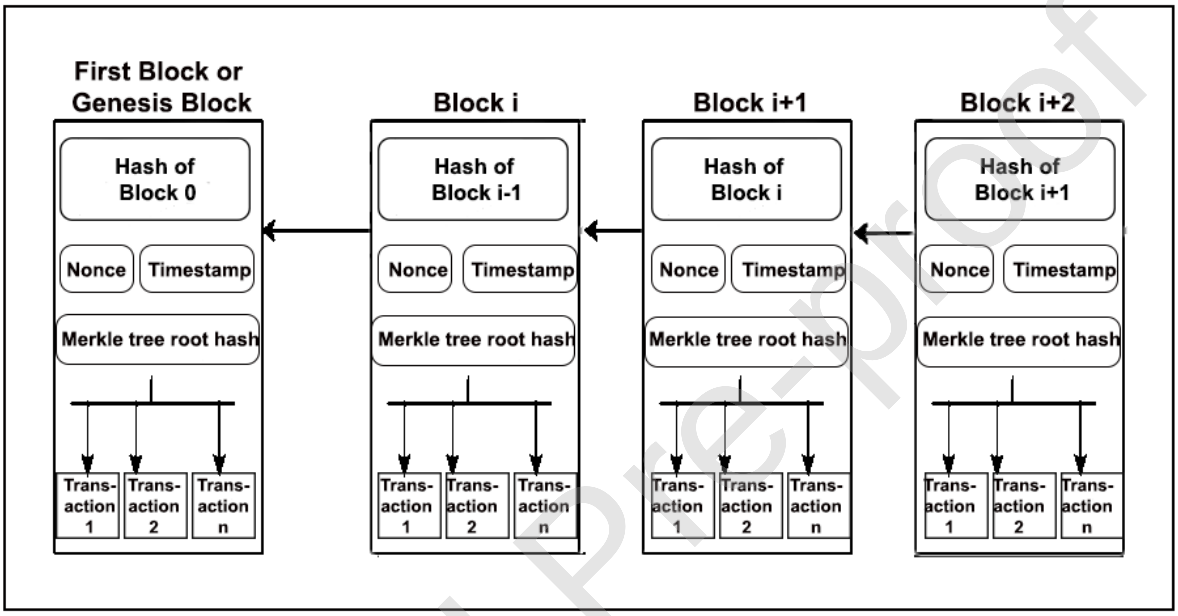


Figure 1: General block structure

2.2 Types of Blockchain

Blockchain systems can be broadly categorized into three types on the basis of control mechanism and authentication namely public, private and consortium blockchain. These types are explored in the subsections below.

2.2.1 Public Blockchain

A public or permission less blockchain is a decentralized open source platform that facilitates every individual to join and perform mining independent of its organization [39]. Every participating node have full freedom to perform operations such as writing, reading, reviewing or auditing of blockchain. Every user in a public blockchain collects the transaction information and initiates the process of mining to earn the reward owing to its transparent nature. The miner node initially collects the transaction information, validates them, initiates consensus mining and finally appends the earned reward with the existing blockchain. The consensus mechanism plays a major role to maintain consistency of blocks throughout the blockchain in order to avert the scenario where no nodes possess multiple blocks that can contradict each other [40]. In general, a public blockchain is vulnerable to the sybil attack as the participants are unknown before mining and every node is given the freedom to create the block [41]. Proof-of-Work (PoW) consensus mechanisms is the most efficient mechanism in terms of overcoming such issues. According to this, the adversary must have 51 % of the total mining power in order to control the transaction. Public key cryptography is employed in blockchain in order to secure transactions where hash value of the user's public key is the address of every user. However, owing to their high computational complexity, public blockchains and PoW mechanism is not suitable for applications that deals with voluminous data [42, 43].

2.2.2 Private Blockchain

A private or permissioned blockchain is a decentralized network that allows private data sharing amongst a specified group of people or within an organization. Selected individual or a dedicated team controls the mining process in a private blockchain thereby restricting the access of unknown or new user, until being invited by some controlling authority [44]. Practical Byzantine Fault Tolerance (PBFT) [45], a deterministic distributed consensus is used to ensure transparency in a private blockchain. Furthermore, only the controlling nodes have the permission to perform transactions in a private blockchain. This property inclines the private blockchain towards the line of centralized architecture but few other properties of private blockchain such as smart contracts, transparent log, distributed ledger and consensus still make sit suitable for banks and other financial organizations [46].

2.2.3 Consortium Blockchain

A consortium blockchain is the merger of private and public blockchain in which a group of individuals take up the responsibility of consensus and block validation decisions. Block in such network is mined with the help of a multi-signature scheme and the miner blocks are considered valid only if it is approved and signed by the controlling node. The major disadvantage of consortium blockchain is its vulnerability against tampering attack. Furthermore, the group of nodes controlling the blockchain can maliciously collaborate to tamper or reverse a transaction thereby threatening the immutability and irreversibility of the blockchain network [47, 48].

Table 3 compares the aforementioned blockchains in terms of their nature, consensus protocols, transaction approval frequency, participant type, permissions, transparency, energy consumption, scalability and efficiency.

Table 3: Comparison of various types of blockchain

Properties	**Public [39, 40, 42, 43]**	**Private [44 – 46]**	**Consortium [47, 48]**
Nature	Decentralized and open	Restricted and controlled	Restricted and controlled
Consensus protocols	PoW, PoS, DPoS	PBFT, RAFT	PBFT
Transaction approval frequency	Long	Medium	Short
Participant type	Resilient and Anonymous	Trusted and Identified	Trusted and Identified
Permissions	Permission less	Permissioned	Permissioned
Transparency	Low	High	High
Energy consumption	High	Low	Low
Scalability	High	High	Low
Efficiency	Low	High	High
Example	• Bitcoin • Litecoin • Dash • Ethereum • Factom • Blockstream	• Ripple • R3 • Hyperledger	• Multichain • Blockstack • Blockchain

2.3 Consensus Protocols

The process of reaching consensus in a blockchain network is a transmutation of the Byzantine Generals (BG) problem in which a group of generals of the byzantine army surrounds an enemy city [49]. The involved generals must agree upon a common line of attack only by communicating via messenger. However, there is a possibility of existence of traitors within the generals who might try to confuse other generals by sending different decisions to different generals. Therefore, in such trust less environment, the main problem lies in finding a solution using which the loyal generals to reach an agreement. Similar to reaching consensus in such an environment, reaching consensus is also a problem in a distributed blockchain network. Various protocols that ensure consensus among ledgers in different nodes are detailed in the subsections below.

2.3.1 Proof-of-Work (PoW)

It is a proof-based consensus algorithm that identifies the node with the right to append the newly mined block to the existing chain in presence of sufficient proof of its effort [50]. When all the nodes or group of nodes broadcast their blocks with similarly verified transactions, there pops up an ambiguity on which node will put the transaction into the block. This issue is resolved by PoW in which the nodes solve a computationally difficult puzzle in order to receive the opportunity of appending the newly created block with the existing chain. All the participants of a decentralized network need to continuously calculate the hash value with the help of different arbitrary value called *'nonce'*. Owing to the difficulty involved in predicting the output values of the hashing functions from the known input values, guessing an acceptable nonce is difficult. After gaining the appropriate nonce, miners broadcast the block where all other network nodes use it to verify the solution. Only after all the miners approve the block, it is appended to the existing chain. This effort put by the nodes in guessing an appropriate nonce value is called the PoW. **Figure 2** depicts the process of block creation in PoW algorithm.

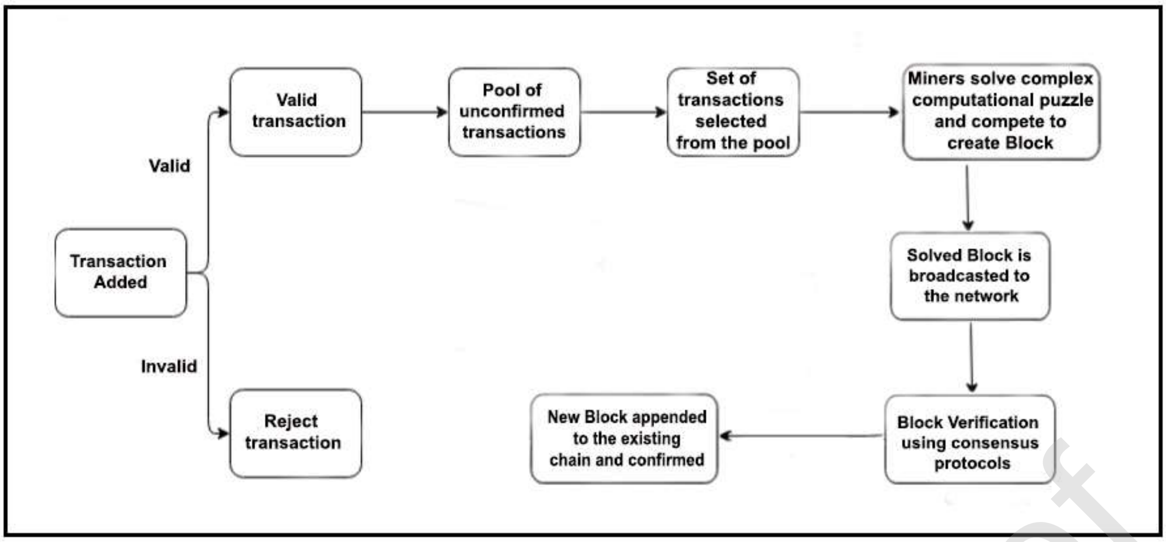


Figure 2: Block creation in PoW consensus protocol

Furthermore, there can also be a scenario in which at the same time more than one miner solves the puzzle and finds the nonce [51]. In such a scenario, all these miners try to broadcast their block along with the calculated nonce in the entire network. This leads to ambiguity among the miners about which block it must consider and append to the current chain resulting in a *"forking problem"*. A fork or branch is generated because the miners verify only the first coming block and ignores all others. PoW employs the *longest chain rule* in order to effectively counter the forking problem. Blockchain forking is depicted in **Figure 3** where two validated blocks (S1 and O1) are generated from a block B simultaneously. Once a new block S2 is appended with S1, the miners working on the fork O1-O2 leaves this block orphaned and immediately switches to S2. In general, a chain is considered successful if a single fork generates at least six consecutive blocks. The main disadvantage of PoW consensus is that it incurs huge computational resource to solve the puzzle and create a block. Furthermore, the process is not sustainable as at the end there will be only one successful miner.

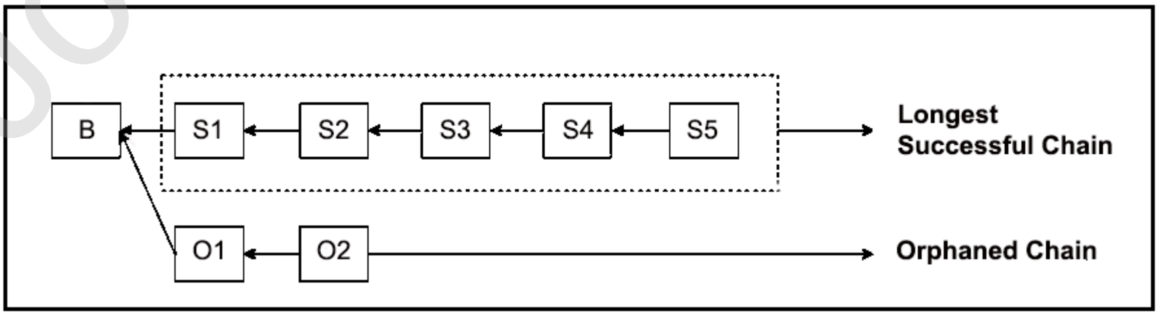


Figure 3: Forking problem in blockchain

2.3.2 Proof of Stake (PoS)

PoS is an energy efficient option to PoW where the miners interested in block creation process relies on having an ample stake in the system instead of wasting their computational resources in solving complex mathematical puzzle [52]. Chances of receiving an opportunity for block validation depends entirely on the wealth of the participating nodes or its stake in the system. Furthermore, a sufficient stake mitigates the possibility of any kind of malicious activity that might be launched on the network [53]. A validator is chosen considering its stake in the network and with the help of this stake it places a bet. After the successful approval of the block, the validators receive the fees. This makes PoS more sustainable than PoW owing to its ability to provide better throughput, latency and energy efficiency. However, there are several drawbacks associated with PoS. Firstly, the wealthier nodes may receive more block validation opportunities as the validators are chosen only on the basis of their stakes. This may enable some nodes to become more dominant in the network thereby resulting in centralization or unfair distribution. Also, the low mining cost requirement as compared to PoW makes this consensus protocol more prone to malicious activities. Nothing-at-stake problem [54] is a recently discovered drawback of PoS and focuses on securing a consensus coordination point without relying on physical reality.

In order to address these issues, several recently proposed PoS protocols such as Ethereum Casper [55], focusses on actively penalizing the validators for malicious activities. King et al. [56] proposed an age-based stake selection algorithm named PeerCoin where larger and older sets are given higher priority for block mining. Vasin et al. [57] proposed the concept of BlackCoin that uses randomized approach to select the next block generator and looks for the size of the stake as well as the lowest hash value. Bentov et al. [58] proposed to ensure uniform, pseudorandom choice of validators by merging the desirable features of both PoW and PoS in the form of Proof-of Activity (PoA). There are several other proposed approaches such as Proof of Deposit (PoD) [59], Proof of Storage (PoSt) [60] and Proof of Importance (PoI) [61] which use deposits, storage and tokens respectively as the stakes.

2.3.3 Delegated Proof of Stake (DPoS)

DPoS is an elective consensus scheme in which every node with a stake in the network employs *'voting'* [62]. In contrast to the direct democratic approach followed by PoS, DPoS follows a representative democratic approach. The stakeholders elect the delegates known as 'witnesses' to generate and validate a block

[63]. These delegates take turns on voting in order to validate previous block authenticity on behalf of their stakeholders. Furthermore, DPoS has significantly lesser number of participants as compared to PoS for the purpose of validating blocks, thereby facilitating faster block generation and quicker transaction confirmation. Also, the network parameters such as block intervals and block size can be finetuned in order to ensure efficiency. However, the centralization tendency of DPoS is its main limitation as the high-stake participants can increase its chance of becoming validators by voting themselves or even by manipulating others to vote.

2.3.4 Proof of Burn (PoB)

PoB is a mechanism to verifiably destroy cryptocurrencies. It consists of two functions. First, a cryptocurrency address generating function in which the money is irrevocably destroyed if the user sends money to this address. Second, a verification function that is dedicated to finding whether an address is really unspendable. The validators in PoB consensus protocol are allowed to create new blocks and earn rewards only if they spend their coins by sending them to an unspendable, verifiable and public address. Apart from solving the energy consumption issues of PoW, the coin burning strategy of PoB also reduces the number of coins on the blockchain thereby gradually increasing the coin value. Other benefits associated with the coin burning strategy includes spending unsold coins, balancing the number of coins and paying the transaction. The burn protocols have the following properties. *Uncensorability*, which mandates that a burn address and a regular cryptocurrency address is indistinguishable; *binding*, which facilitates association of a metadata with a particular burn; and *unspendability*, which refers to not spending the address that has been correctly verified as a burn address.

2.3.5 Proof of Elapsed Time (PoET)

PoET was first proposed by Intel for blockchain construction based on its trusted computing platform SGX (Software Guard Extensions) [64]. The basic working principle is that each node generates a random number in order to estimate its waiting time before it is given the opportunity to generate a block. In contrast to all other consensus protocols, PoET choose a leader in the chain to create new blocks instead of all users being involved in the validation process. In order to elect the leader, a random timer is associated with every node on the network and the node with minimum expiry is selected as a leader [65]. As the random leader election algorithm is executed continuously in PoET consensus mechanism, it eases to trace the malicious user in case the same nodes are elected as a leader every time.

2.3.6 Proof of Capacity (PoC)

Owing to the need of finding random nonce values for the purpose of block unlocking, the traditional PoW protocols become computationally intensive. PoC is an alternative solution to such issues that utilize the hard drive space of the nodes in a blockchain network. Instead of randomly generating the nonce values, all the possible nonce values are stored on the hard drive and while unlocking the blocks, the matching nonce-hash pairs are selected [22]. The nodes that possess more disk space receives more stake in PoC consensus protocol.

2.3.7 Practical Byzantine Fault Tolerance (PBFT)

A condition in which consensus is safely reached between two communicating nodes across a distributed network even in presence of few misbehaving nodes is referred to as Byzantine Fault Tolerance (BFT) [66]. PBFT, a replication algorithm designed to serve as a high-performance consensus protocol is the most widely accepted example of BFT. The nodes in PBFT are sequentially ordered with one leader and others serving as backups. Whenever a request is received by the leader nodes, it passes it to the backup nodes for further processing. The leader nodes also serve to send the result to the request originator [67, 68]. The decisions in PBFT are made considering the majority votes where every node communicate among themselves in order to prove the integrity as well as origin of the message. The entire process of PBFT is realized in three phases namely *pre-prepared, prepared* and *commit*. In all these three phases, a node would move to the next phase only if it receive votes from two-third of all the nodes in the network. This enables the PBFT consensus mechanism to run effectively even under presence of few malicious byzantine replicas. Mazieres et al. [69] proposed a byzantine-based consensus protocol named Stellar Consensus Protocol (SCP) in which the nodes possess the right to choose the set of participants it must believe. Nasreen et al. [70] studied various BFT methods in distributed networks and tried to solve the problem of broadcasting messages reliably in a multi-hop network. Rakitin et al. [71] proposed a distributed, semantic-driven consensus protocol to provide resistance to byzantine errors and preserve data localization.

2.3.8 Proof of Authority (PoA)

PoA is a family of consensus protocol especially designed for permissioned blockchain. It achieved significant performance gains over the typical BFT algorithms in terms of lighter messages being exchanged over the network. The high energy consumption problem as well as the problem of dependency in PoW consensus algorithm is solved by the PoA protocol which requires the validators to have monetary stake on the blockchain. In PoA consensus protocols, the authoritative control is delegated to specific nodes that exploit the criteria of majority votes to form the consensus and create new blocks [72]. PoA considers *N* trusted nodes called *'authorities'* for running a consensus and assumes atleast $\left(\frac{N}{2}+1\right)$ of them to be honest. A widely used approach named *mining rotation schema* is the basis of consensus in PoA and is mainly required for fair distribution of block creation responsibilities among authorities [73, 74]. Originally proposed as an essential component of Ethereum ecosystem suited for private networks, PoA was implemented into clients Aura (Authority Round) [75] and Clique [76]. The two implementations of PoA consensus algorithm works in different manner. Even though both have a similar first round of *block proposal* in which the current leader proposes a new block, these differ in the fact that Aura requires an extra round of *block acceptance* which is not mandatory in clique. The latency of Aura in terms of message rounds is $\left[2*\left(\frac{N}{2}+1\right)\right]$, as the block is committed only after being proposed by majority of authorities (say *N*).

2.3.9 Raft

Raft is a voting-based consensus scheme proposed to make Paxos algorithm more implementable and understandable for practical scenarios. The original Paxos algorithm aims to overcome the consistency issues related to byzantine general problem [77, 78]. Both Paxos and Raft achieve similar efficiency and are non-byzantine fault tolerant algorithm. Raft relies on two major operations namely leader selection and log replication. The leader manages the ordering of transactions and in case the existing leader fails, new leader is selected using randomized timeout. The log replication phase is triggered in which the leader accepts log entries from clients and creates its own version of transaction log by broadcasting the accepted log entries [79]. Quorum and Corda are the implementations of blockchain that employs Raft as their consensus algorithm. Generally, Raft achieves low latency and high throughput. However, the overall performance of this consensus scheme depends on the performance of the leader which enjoys an absolute dominance in the system. Furthermore, it is capable of enduring crash faults of up to 50 % and the entire system can be compromised if the leader node gets maliciously infected. Therefore, restricted throughput and high security risks make it unsuitable for smart city applications.

2.3.10 Ripple

Ripple [80] is an open-source payment protocol that makes use of collectively trusted subnetworks within large-sized network. Ripple aims to decentralize payment, currency exchange and clearing functions. Nodes in the network are divided into two types: a client that transfer funds and a server that participates in the consensus process. Transactions within the network is initiated by the client and the validating nodes or tracking nodes broadcast these to the entire network. These validating nodes are responsible for responding to the client's ledger request as well as distributing transaction information. In Ripple, consensus is achieved between the validating nodes that are comprised of several trusted nodes called Unique Node List (UNL). It works under assumption that any two UNL cliques (say UNL_i and UNL_j) are 20 % overlapped such that at least $\frac{1}{5}\left[max\left(UNL_i|UNL_j\right)\right]$ inter-clique UNL relationship is shared. Ripple is more efficient as compared to other anonymous consensus protocols such as PoW because the identity of the participating nodes is known in advance. These are more suited for permissioned blockchains and can achieve fault tolerance of 20 % without affecting the normal consensus operations.

Table 4 compares the aforementioned blockchain consensus protocols in terms of their background, language used, resource consumption, processing speed, energy efficiency and limitations.

Table 4: Comparison of various consensus protocols

Consensus Protocol	**Background**	**Language**	**Resource Consumption**	**Processing Speed**	**Energy Efficiency**	**Limitations**
PoW [50, 51]	Nodes solve a computationally difficult puzzle in order to receive mining opportunity.	Solidity, C++, Golang	High	Slow	Low	High power consumption and Less secure
PoS [52]	Chances of receiving an opportunity for block validation depends on its stake in the system.	Native	Low	Fast	High	Highest paid stakeholders enjoys consensus control

DPoS [62, 63]	Every node with a stake in the network employs *'voting'*.	Native	Low	Fast	High	Constraints on the number of token holders
PoB	Coin burning strategy.	Solidity, C++, Golang, Serpent	Medium	Medium	Low	Resource wastage
PoET [65]	Each node generates a random number in order to estimate its waiting time	Python	High	Medium	High	Same nodes are elected as a leader every time.
PoC	Utilize the hard drive space of the nodes.	-	High	Slow	High	Nodes with more disk space receives more stake
PBFT [66 – 71]	The decisions are made considering the majority votes where nodes communicate in order to prove the integrity and origin of the message.	Java, Golang	High	High	High	High communication overhead
PoA [72]	Requires the validators to have	Java, Solidity	High	Medium	Low	Scalability issues

	monetary stake on the blockchain.					
RAFT [77 – 79]	Voting based consensus scheme that elects leader using randomized timeout and performs log replication to achieve consistency in BFT environment.	C++, Java, Scala, Go	Medium	Fast	High	Restricted throughput and low security
Ripple [80]	Uses collectively trusted subnetworks within single large sized network.	C++, Java	Medium	Fast	High	No incentive for nodes and no transaction limit.

2.4 Architecture of Blockchain

Blockchain operates in a decentralized environment supported by several core technologies including distributed consensus algorithm, cryptographic hash and digital signatures. In general, the blockchain architecture is composed of six main layers namely the data layer, network layer, consensus layer, incentive layer, contract layer and application layer as depicted in **Figure 4** [81 – 83]. A detailed description and function of these layers are presented in the sub sections below.

2.4.1 Data Layer

This layer supports features for manipulating a variety of data aggregated from social, physical and cyber spaces [84, 85]. The main responsibility of this layer is to encapsulate the time stamped data blocks. Verified transactions are stored in the block body whereas the block header contains the metadata, timestamp, Nonce, Merkle root and hash of current block. The current block uses the hash of the previous block (parent block) in order to connect with its previous block. The creation time of the block is indicated by the timestamp. In this layer, time stamp and Merkle tree are the two important components for the blockchain ledger. Time stamp enables precise positioning and traceability of the blockchain data. It can also endow blockchain data with a time dimension so as to facilitate recurring of past data history. The Merkle tree store the transactions within some specified time period via hash binary tree in order to efficiently verify the integrity and existence of these transactions.

2.4.2 Network Layer

The main responsibility of the network layer is to verify, forward and distribute blockchain transactions. Therefore, this layer is provided with data verification mechanism, communication mechanism and distributed networking mechanism [86, 87]. Majority of blockchain based applications involve dynamic and open environment with numerous distributed and connected devices. Generally, the blockchain network topology is modelled similar to a P2P network having equally privileged peers as participants. A transaction after being generated is broadcasted to all the neighbouring nodes that verify these based on some predefined specifications. A transaction is forwarded to other nodes only if it is valid else it is discarded. In order to verify the transactions authenticity, asymmetric cryptography based digital signature mechanism is employed [88, 89]. Digital signature operates in two phases: Signing phase in which a node after creating their transaction signs them using its private key; and the Verification phase in which the authenticity of the received transaction is verified using the initiator's public key.

2.4.3 Consensus Layer

In a decentralized environment, efficiently reaching consensus amongst the untrustworthy nodes is an issue of paramount concern [90]. Owing to the absence of any trusted central authority, there is a need of some protocol capable of ensuring consensus among the decentralized nodes. The most prominent consensus mechanisms in the existing blockchain systems include PoW [50, 51], PoS [52], DPoS [62, 63] and PBFT [64, 65]. In PoW consensus algorithm, nodes run hash functions in order to generate a nonce vale that eases the validation process by other nodes. In PoS consensus algorithm, the nodes possessing the highest value of stake are allowed to generate blocks. DPoS is almost similar to PoS with an only exception that it is representative democratic while PoS is direct democratic. PBFT consensus protocol is a byzantine fault tolerant replication algorithm. Some other less popular consensus protocols include PoET [64, 65], PoC [22], PoA [72], Proof of Retrievability (PoR) [91], Proof of Trust [92] and Proof of Luck [93].

2.4.4 Incentive Layer

The main responsibility of the incentive layer is to integrate the economic factors such as allocation mechanisms and economic incentive issuance into the blockchain network. The competition driven block creation and data validation process can be considered as a crowdsourcing task in which the self-interested nodes contribute their power. Some economic incentives (such as digital currencies) is issued as reward which needs to be distributed to the corresponding nodes based on their contributions. The designed incentive mechanism must promote individual revenue maximization and guarantee trusted and secured ecosystem [94, 95]. This is considered as the major driving force for the blockchain network as it motivates the nodes to carry out data verification. Apart from serving as an engine for powering blockchain, such incentive mechanisms also establish an embedded, cryptocurrency based financial system to support real-time micro-payment and disintermediated trading. Furthermore, incentive layer is optional for partially centralized blockchain applications that requires mandatory participation of trusted entities without payment or financial requirements.

2.4.5 Contract Layer

The contract layer focusses on enabling complex programmable transactions in a blockchain utilizing smart contracts, algorithms and various scripts. A group of state-response rules called smart contract is used to express business logic, control digital assets, and formulate the rights and obligations of the participants. If two or more participants agrees onto all the terms within a smart contract, the contract is cryptographically signed and broadcasted to the entire network [96]. The smart contracts execute automatically and independently according to the predefined rules once these conditions are met. Similar to transactions in a blockchain, a smart contract is a self-executing program whose inputs, outputs and states are verified by every node in the network. For implementation of a transaction logic, every blockchain systems use their own programming language. Non-

Turing complete languages are used by Bitcoin and its derived altcoins for validating the availability and ownership of the cryptocurrencies. Also, the developers are provided with approximately 200 opcodes by Bitcoin that enables them to write their stack-based programs. However, Ethereum uses Turing complete languages (e.g., Solidity [97]). Ethereum Virtual Machine (EVM) is required to compile the smart contracts into low level bytecodes which can be broadcasted to Ethereum blockchain network [98].

2.4.6 Application Layer

Application layer is the one where the client or end user is located. The client application initiates a transaction in order to kickstart a business workflow. This layer constitutes the central user interface for distributed ledger technology that provides products and services. It comprises of various business applications such as digital identity, market security, intellectual property, Internet of Things (IoT) and so on [99, 100]. The application can use a language specific Software Development Kit (SDK) or a command line interface tool provided by the blockchain implementation to communicate with the network nodes. These application helps to optimize business management and provide new services. Application layer encompasses frameworks, user interfaces, APIs and scripts that are utilized by the end users to interact with the blockchain network. It has a sublayer named execution layer that has the actual code and rules that are executed.

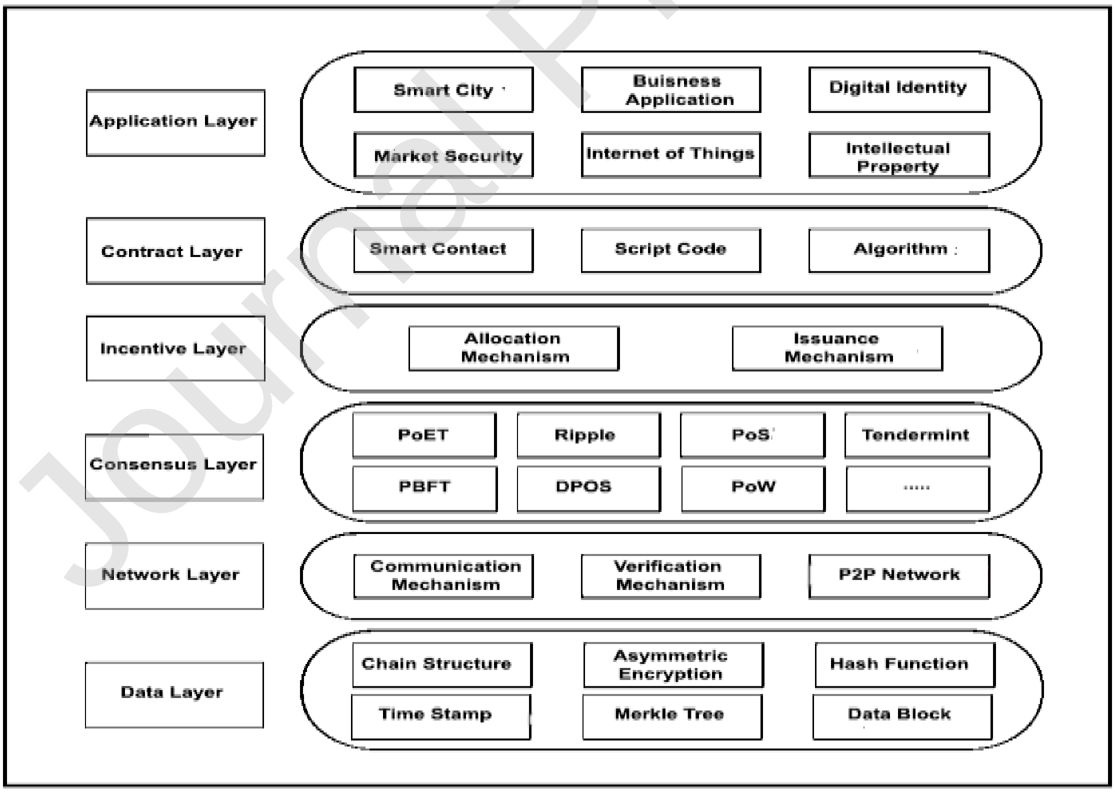


Figure 4: The layered blockchain architecture

3. Smart City: Characteristics, Pillars and Security Requirements

Smart city refers to the concept of applying all the available resources and technologies in a coordinated manner aiming to develop an integrated, habitable and sustainable urban centres. Some well-known applications of smart city in modern societies include smart energy for optimizing consumption; smart building capable of independently commanding the energy consumption, lighting system and security throughout; smart technology for enabling edge processing solutions and intelligent network connectivity in cities; smart mobility for licensing intelligent mobility, smart healthcare for enabling connected medical devices and intelligent systems to promote diagnostics, health monitoring and wellness; smart security for mitigating security risks to protect information, properties and even people; and smart governance for providing digital services and policies from the government [101 – 103]. Constructing a smart city for saving valuable resources and time requires high degree of network connectivity which might result in security vulnerabilities. IoT devices that collect data from various sources and transfers them to a central storage location deteriorates this problem further. These extend the attack surface by creating an entry point for adversaries facilitating their intrusion into the system [104, 105]. These adversaries can degrade the quality of intelligent services by launching wide range of attacks such as session hijacking, Structure Query Language (SQL) injection [106], Denial of Service (DoS) [107, 108], eavesdropping [109] and brute force attack [110]. Smart city comprises of attributes (characteristics), themes (pillars that enable its continuous progression) and infrastructure (to provide the operational platform). These aforementioned features of smart cities are explored in the subsections below.

3.1 Characteristics of a smart city

A smart city is built upon several attributes including sustainability, smartness, urbanization and QoL (Quality of Life). Sustainability is the premier paradigm in urban development and the emergence of smart cities is an outcome of prevalent attention on sustainability. Mohanty et al. [111] proposed to add few sub attributes such as social issues, economics, infrastructure and governance, energy and climate change, pollution and waste, and health to sustainability. There is a drastic increase in the utilization of natural resources by the cities of modern world therefore scrutinizing the consequences of exhausted non-renewal energy sources is of utmost importance. Jong et al. [112] highlighted the need to maintain sustainability of smart city by safeguarding energy sources and natural heritages. The ability of a city to perform its operations and uphold the balance of ecosystem in all the aforementioned departments is known as *sustainability*. The desire to improve the overall social, economic and environmental benchmarks of the city is referred to as *smartness*. *QoL improvement* is indicated by the financial and emotional well-being of urban citizen. Infrastructural, economical, technological and governing aspects that are involved in the transformation of rural to urban environment is known as *urbanisation*. Interdependence and interrelationship between these sub attributes are shown in **Figure 5.**

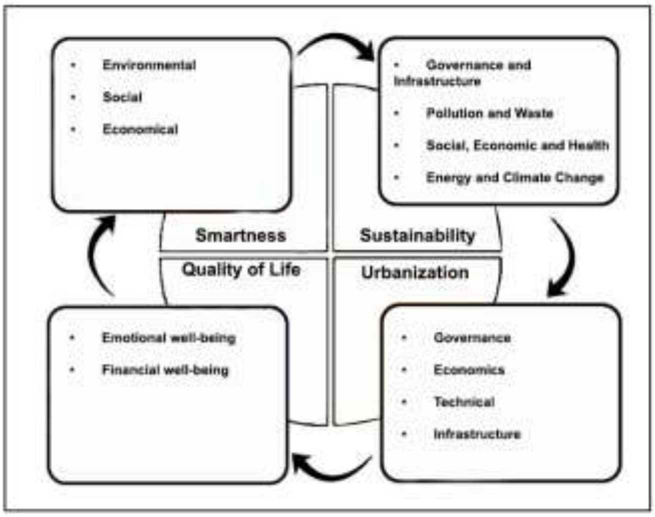


Figure 5: Characteristics of a smart city

The concept of smart city was initially proposed to improve the QoL level of citizens using various innovative solutions that reduces the social participation barriers and social learning restrictions. Nowadays, well-defined social policies are introduced by the modern city councils to employ skilled citizens for upgrading the provisions for quality of city service. Therefore, the QoL enforcement must satisfy emotional and financial well-being of both citizens and employees. For an instance, healthcare service campaigns were established in Chicago in order to upgrade the services offered to the less privileged citizen groups in the city [113]. Similarly, an artists' circle was implemented in the City of Yokohama, Japan in order to assemble artists and organize performances, workshops and exhibitions [114].

Smart cities are perceived as the emerging urban utopias by the modern world [115]. Researchers realized smart city as a perfect solution to counter the problems arising from drastic urbanization such as traffic congestion, adverse human health, air pollution, waste management predicament and resource scarcity. Caragliu et al. [116] studied the correlation between smart cities and urbanization in Europe by identifying numerous factors that had positive influence on urban wealth. These factors include the use of ICT in public administration, accessibility to ICT, level of education and attention to urban environment. Shi et al. [117]

investigated the relationship between urbanisation and the rate of carbon emission in various cities of China. They noticed that in case of high rate of urbanisation, the three-stage curve shows shape of negative increase, positive decrease and positive increase. Whereas, in case of low urbanisation rate, the three-stage curve shows shape of negative decrease, positive decrease and positive increase. Finally, it was concluded that under varying urbanisation stages, there is a significant difference in carbon emissions. Silva et al. [118] studied the essence of sustainable smart cities and presented several technological, governing and economical barriers that hampered evolution of smart city into a mainstream throughout the globe. Sun et al. [119] proposed that better adaptation to climate change in urban environment requires local "climate-smart" strategies such as rational use of green planning and mitigating the local anthropogenic heat emissions.

3.2 Pillars of Smart City

Smart city is believed to be based upon four themes/pillars namely physical infrastructure, institutional infrastructure, social infrastructure and economic infrastructure. The main responsibility of these aforementioned pillars are as follows.

- *The physical infrastructure* aims to ensure resource sustainability and smooth city operations. It comprises of manufactured infrastructure and natural resources. Smart city is realized with the help of quality smart object network and ICT infrastructure. The physical infrastructure is also extended to smart energy, renovation of buildings, green urban planning and green buildings.
- *The institutional infrastructure* serves to enhance the smart city governance by participating in decision making, political strategies, transparent governance and social services. It is essential to gain maximum benefit of the human capital and work with the citizens for easy governance as well as betterment of the city. The institutional infrastructure collaborates with the central as well as regional government for exploiting maximum benefit from the smart city. It integrates national, civil, public and private organisations in order to provide necessary interoperation between services. Kitchin et al. [120] proposed technocratic governance to be a driving force for institutional infrastructure as it presumes that all the features and services of the city can be addressed using technical solutions.
- *The social infrastructure* is comprised of human capital, QoL and intellectual capitals. Social infrastructure helps to maintain sustainability in a smart city as citizen awareness, popularity and commitment contribute towards making the concept of smart city popular [121].

- *The economic infrastructure* refers to the steady growth of the economy and jobs so as to escalate the city productivity by utilizing best practices of e-business and e-commerce. Lombardi et al. [122] investigated this aspect using a modified triple helix model and several performance indicators such as gross inland energy consumption indicator, employment rate in various industries, GDP per head and projects funded by civil societies.

3.3 Security requirements of smart cities

ICT have played an important role in almost every aspect of our daily life ranging from education, health and personal lives to national security. Majority of government projects adopted smart city programs in order to manage issues related to health, water, energy, transportation, surveillance and security. In addition to making our life easier, the smart cities also bring forth several security challenges because of increasing interdependency, connectivity and complexity among them. In order to securely implement the smart city, a clear understanding of these challenges is of utmost importance. In this section, we explore the most prominent requirements that needs to be taken care of in order to build a secure smart city.

3.3.1 Secure Communication

Smart city architectures rely heavily on network communications for joining different components in order to collect, share and transfer data throughout the smart city. Securing wired as well as wireless communications in a smart city requires to guarantee the basic security principles such as confidentiality, integrity, authentication and non-repudiation [123, 124]. Employing lightweight cryptographic schemes for encryption, decryption and creation of shared secret keys is an acceptable way to secure smart cities communications. Several works have been proposed in this regard. Li et al. [125] proposed a public key encryption based novel lightweight mutual authentication scheme aimed to balance communication cost and efficiency without compromising the security in smart city applications. Similarly, Mick et al. [126] proposed a scalable lightweight authentication framework suited for Named Data Networking (NDN) projects that provides in-network caching, stateful forwarding and built-in data provenance assurance to IoT applications. In another work, Mahmood et al. [127] proposed a lightweight Elliptic Curve Cryptography (ECC) based authentication scheme for smart grids that withstands security attacks and guarantees mutual authentication incurring low communication and computation cost. Similarly, Lara et al. [128] proposed binary Edward curves based lightweight ECC accelerator to meet the cost and efficiency requirements of various IoT applications. Similarly, Hammi et al. [129] proposed to extend the concept of traditional One Time Password (OTP) authentication scheme by using ECC to ensure IoT security. Apart from using OTP for initial authentication, the proposed scheme generates a new One Time Key (OTK) for signing the communication. This approach achieved improved security and overall performance without relying on any challenge-response scheme or timestamp. Luo et al. [130] proposed a symmetric key based communication protocol that relies on ultra-lightweight encryption standards for safeguarding data transmissions. In another work, Zhang et al. [131] proposed a lightweight PHY-layer authentication system that relied on tag verification and tag embedding. The proposed framework aimed to prevent malicious users from forging authentication tag and thereby preventing attacks such as man-in-the-middle, tampering and unauthorized detection. However, employing such security algorithms in smart cities is a challenge due to heterogeneity of the connected devices.

3.3.2 Secure Monitoring and Response

Monitoring strategy is an essential requirement for any system dedicated towards detecting anonymous behaviour and controlling the surrounding environment. IoT devices responsible for collecting and transferring data is vulnerable to attacks like injection of erroneous or fake sensor data. In order to respond to a doubtful behaviour or an attack, the system must consider elimination or response strategies. In elimination strategy, the system must completely remove or temporarily isolate the affected parts of the IoT device whereas the response strategy considers a formal incident response process to counter the vulnerability. Such monitoring response system was first designed by Cisco that provided recommendations for threat mitigation utilizing the concept of incident management. However, the applicability of the proposed system is limited only to Cisco network equipment [132].

3.3.3 Secure Booting

Worms, viruses and other malwares reside as an executable code and have the capability to be distributed via internet connection. This helps them to overwhelm the target systems via boot sectors. Pre-boot malware takes over the control of the system and hides itself in such a way that it is not even detected by virus scanners or the Operating System (OS) kernel. In such scenarios, the cryptographic hash based secure boot technology guarantees the authenticity and integrity of the software packages by avoiding execution of unsigned code. However, majority of the proposed secure booting techniques were inapplicable for IoT devices due to their constrained processing resources. Therefore, an ultra-low power consuming hash function based efficient boot securing design for IoT devices is proposed [133].

3.3.4 Application Lifecycle Management

Smart cities rely heavily on IoT devices for facilitating data collection, data analysis and interaction with the citizens. Therefore, it is necessary to predict actions and plans needed for such devices. The life cycle management of IoT devices is directly related to device management, identity management, software and application development. Therefore, apart from considering security measures at every service level, the developer must also validate the key, code and system components at every stage of installation and development. Sinaeepourfard et al. [134] proposed Smart City Comprehensive Data Life Cycle (SCC-DLC), a novel cloud and fog architecture-based data management model aimed to manage the voluminous data collected during various phases of smart cities lifecycle.

3.3.5 Updating and Patching

Software updates are necessary for IoT devices to overcome complex security attacks by identifying and addressing the vulnerabilities efficiently. Furthermore, an IoT device must possess intelligence to authenticate the patches received from their service providers and operators [135]. However, the authentication process must not degrade the functionality of the IoT device and also the security patches must be present in a compressed, downloadable format in order to prevent bandwidth wastage [136]. In addition to serving as an effective countermeasure against the cyber-attacks, the process of updating and patching is also a challenge for several IoT devices. This is majorly because the medical device manufacturers have little or no experience of dynamic patch update. This problem also deteriorates further due to restrictions posed by drug and food administration, which makes the process of medical device updation more time consuming and rigorous.

3.3.6 Authentication and Access Control

Controlling and managing the data generated by the IoT devices and at the same time preventing unauthorized access is essential for IoT systems [137]. Smart cities must be capable of preventing unauthorized access by maintaining access control, constructing secure communication and authenticating the IoT systems. In order to guarantee data privacy in cloud-based smart cities, several access control and authentication protocols have been designed such as Identity Based Encryption (IBE) [138], Role-Based Access Control (RBAC) [139] and Attribute Based Encryption (ABE) [140]. These protocols help the smart cities to handle the authorized users as well as revoke their permission rights [141].

3.3.7 Application Protection

In a typical smart city, there is a need to leverage multiple methods simultaneously in order to identify system vulnerability and guarantee protection against various types of attacks that might be launched in a smart city. Several existing schemes can be used to secure the IoT device applications. For an instance, the privacy of smartphone applications can be preserved by securing the International Mobile station Equipment Identity (IMEI), Mobile Equipment IDentifier (MEID) and Unique Device Identifier (UDI) of smartphones. Apart from this, existing cryptographic primitives and key management schemes can be employed to protect the communication links thereby enabling secure data transfer among various components of smart cities.

Table 5 compares the aforementioned security requirements for smart cities in terms of the solutions proposed to meet the security requirements and the challenges faced in adopting these solutions.

Table 5: Comparison of security requirements for smart city

SI. No.	Security requirements	Solutions proposed	Challenges faced
1.	Secure Communication [123 – 131]	Lightweight cryptographic schemes	Heterogeneity of devices connected together
2.	Secure Monitoring and Response [132]	Cisco designed Monitoring, Analysis and Response System (MARS)	Suitable only for Cisco network equipment
3.	Secure Booting [133]	Cryptographic hash based secure boot technology	Inapplicable for majority of the IoT devices
4.	Application Lifecycle Management [134]	SCC-DLC [134]	Lack of privacy measurement
5.	Updating and Patching [135, 136]	Linux and Microsoft patch updates	Not applicable for older IoT devices
6.	Authentication and Access Control [137 – 141]	IBE [138], RBAC [139] and ABE [140]	High computation cost
7.	Application Protection	Securing communication links with the help of cryptographic schemes	Lack of security frameworks to provide security at all the layers of smart city architecture.

4. Motivations Behind Applying Blockchain Technology to Smart Cities

Nowadays, smart city projects are gaining popularity and numerous countries as well as cities such as Madrid, Manchester, Barcelona, Amsterdam and Singapore, are actively planning their smart city strategies. Several smart city testbeds are also developed in order to simulate and evaluate the proposed smart city solutions [142]. These test-beds are listed as follows.

- SmartSantander [143] is a commonly known smart city testbed and has successfully deployed 2000 IoT devices, 2000 joint QR code/RFID tag labels, 200 GPRS modules and 400 parking sensors in the city of Santander, Spain. Furthermore, it implemented 8 use cases including traffic intensity monitoring, mobile environment monitoring, environment monitoring, free parking, outdoor parking management, participatory sensing and augmented reality.
- City of Things [144] is another smart city testbed located in the city of Antwerp, Belgium. It facilitates validation of new smart city experiments both at user and technology level. It follows an integrated approach and allows experimentation on three levels namely data level, user level and network level.
- Cyber Security centre in New York University Abu Dhabi (CCS-AD) developed NYUAD [145], a smart city testbed aiming to provide real-time and realistic smart city environment. Such environments can be exploited by the researchers for evaluating their proposed models.
- Cardone et al. [146] developed a testbed in ParticipAct Living Lab at University of Bologna that involved monitoring of 300 students over the course of one year for conducting Mobile Crowd Sensing (MCS) experiments.

In spite of these smart city testbeds, there exists numerous challenges that needs to be addressed before implementation and deployment of smart cities.

4.1 Why Blockchain?

Apart from several non-technological factors (such as skilled human resource requirement and high financial investment), implementation and deployment of smart cities also face several technological challenges. These technological challenges are listed as below.

- In order to improve the city management and provide effective public services to the citizens, there is a need for efficient data collection and analysis. Furthermore, data integrity and reliability are of utmost importance as unauthorized data modification might lead to disastrous consequences.
- The application's complexity and the number of devices in smart cities are increasing exponentially with time. Furthermore, nodes and the devices in smart cities demand some degree of flexibility so that they can join or leave the network anytime based on their requirements. To this end, the decentralized systems are more suitable than traditional centralized systems for smart cities as it offers some degree of fluctuation in the complexity of application and the number of devices being connected.
- Citizens in a city have strong affinity for transparency, democracy and participation. Therefore, the government must convey certain information to them, such as decision-making process, environmental information and government affairs information. The sharing of data such as personal data of citizens, organizational data and IoT data, can improve the decision making and city management.

Blockchain technology possess the following inherent features that makes it an attractive solution to counter the aforementioned challenges in the smart cities.

- *Decentralization:* Transactions are inherently endorsed or trusted in a traditional centralized system via central trusted intermediaries. The use of a central server degrades the overall performance and also incurs additional cost. The blockchain systems does not require a centralized third party to operate in a P2P manner. Public blockchains operate in a fully decentralized environment and allows to establish trust among untrusted or unknown nodes. Whereas, private blockchains operate in a trusted, closed environment and employs various access control schemes to achieve the desired level of trust. Similar to private blockchain, permissioned blockchains also operate in a trusted environment but possesses slightly higher degree of decentralization as these rely on various consortium policies for granting membership status to the nodes. Thus, it is evident that all blockchains exploit the benefits of decentralization in varied proportions thereby preserving data integrity and eliminating the single point of failure [147].
- *Immutability:* Any general centralized database is vulnerable to hacking and requires a trusted third party for preserving security. Blockchain is made immutable and secure using cryptography. All transactions are signed with the help of digital signatures and the data blocks are securely linked via one-way cryptographic hash functions. This function accepts input of any length and generates a fixed

length string as output (called hash). As the immutability of the shared ledger is presented as slight change in the input reflects a serious change in the hash output and data tamper in any block reflects a change in all the subsequent blocks of a blockchain [148].

- *Democracy:* Before including a block into the existing blockchain network, all decentralized nodes execute consensus algorithms to reach to an agreement in a P2P manner. Thus, all nodes in a blockchain network contributes to the decision-making process making it democratized [149].
- *Pseudonymity:* Each node in the blockchain system is assigned a pseudonymous address which helps to hide the real-world identity of these nodes. Inherent pseudonimity is especially essential for the use cases that require the user identities to be private.
- *Security and Transparency:* As finding a single point of failure in a blockchain systems is a tedious task, the network security of the overall system is enhanced. Furthermore, the transparency in a blockchain system is maintained as all the transaction records are accessible for everyone in a blockchain network.

Owing to these merits, blockchain technology can enable transparent city management, ensure data integrity, encourage joint decision-making process among individuals as well as organizations (e.g., universities, hospitals, companies, national and local government), and promote the deployment of a democratized smart city.

4.2 When Blockchain?

Nowadays, several cities including Chile, Santander, Antwrep, Dubai, Vishakhapatnam and Stockholm have successfully launched blockchain-based projects. Sharma et al. [150] proposed a hybrid network architecture for smart cities that utilized the concept of blockchain technologies and Software Defined Networking in order to inherit the strengths of both distributed and centralized network architectures. In another work, Dagher et al. [151] proposed Ancile for efficient, interoperable, and secure access to medical records by providers, third parties and patients. It uses smart contracts for obfuscation of data and heightened access control. Similarly, Li et al. [152] developed a blockchain based networked microgrids to optimize the physical and financial operations of power distribution systems. It stresses on the role of blockchain technology in the evolution of active distribution networks from the traditional power distribution systems. Dorri et al. [153] proposed a Lightweight Scalable Blockchain (LSB) for providing end-to-end security and optimizing IoT requirements. Tanwar et al. [154] proposed to integrate blockchain technology and healthcare industry by designing an electronic healthcare record system that facilitates easy access to patient medical records, hospital assets and prescription database. In another work, Lopez et al. [155] proposed a Blockchain-based Smart Mobility Data-market (BSMD) framework to address the challenges related to scalability, secure management and privacy. Sun et al. [156] proposed to employ blockchain big data platform for construction of smart city in Hefei that facilitates green environment and low carbon emission.

Blockchain has the potential to be applied to huge range of applications. It can be implemented for finding solutions in various domains including supply chain, governance, identity management, voting, healthcare, energy resources and so on. Blockchain solutions are also inherently suited for numerous industrial processes. Furthermore, government core functions and financial services are also aligned with blockchain capabilities. **Figure 6** depicts a simplified flow diagram that can serve as a reference for deciding whether blockchain technology can be applied to a particular application or not.

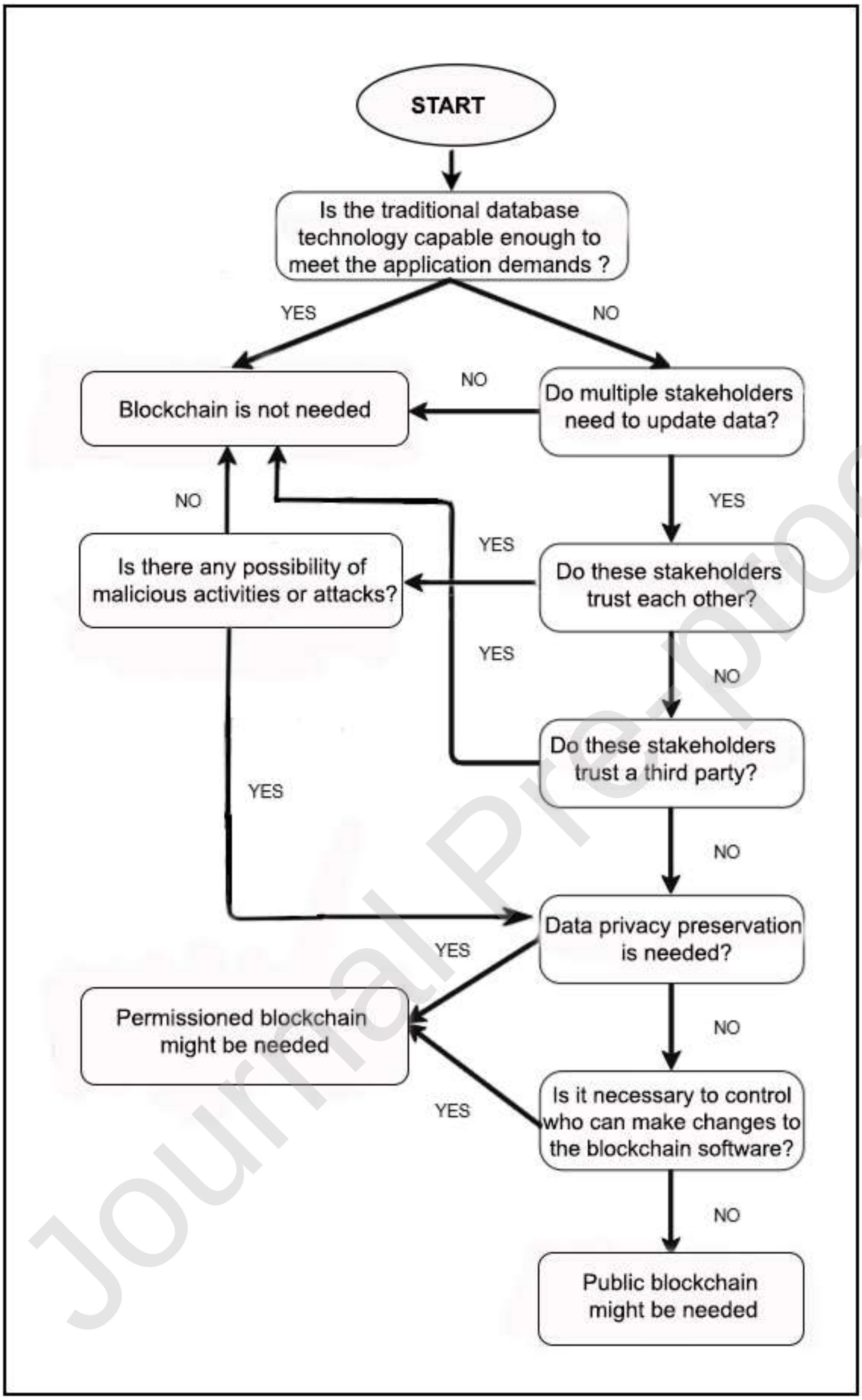


Figure 6: Flow diagram depicting the applicability of blockchain for various applications

5. Blockchain in Smart Cities

There are numerous aspects of smart cities such as smart healthcare, smart transportation, smart grid, supply chain management, financial systems and data centre networks. In this section, we review existing blockchain efforts in each of these aforementioned aspects. This will provide the readers with an insight on how blockchain technology is being applied in the realm of smart cities.

5.1 Smart Healthcare

A typical healthcare network comprises of a group of hospitals that is owned, managed and sponsored by a central authority [157]. But, these centrally controlled healthcare networks are subject to a single point of failure. Furthermore, due to rapid urbanisation of the world's population, meeting the citizens demand is a challenging task for the traditional healthcare systems. This contradiction between the limited resources and the ever-growing demand brings forth the need for an efficient, intelligent and sustainable healthcare. Blockchain technology is the best solution known to provide the desired level of decentralization in healthcare networks and thereby enhance its security.

The realization of smart healthcare is dependent on several components such as smart ambulance systems, smart hospitals, wearable devices and emergency response. For an effective treatment, the patient's data sharing is very important as it may help doctors to make real time decisions related to patient's health by judging their conditions even in remote locations [158]. Blockchain also facilitates storing the medical data in an immutable and secure manner. Also, it eases patients to flexibly manage access to their medical data. The steps involved in the use of blockchain for securing healthcare networks is depicted in **Figure 7** and are listed below [159].

- Step 1: IoT sensors collect and monitor the patient's health information such as pulse rate, blood sugar level, heart rate, respiratory rate, blood pressure, body temperature, etc.
- Step 2: The administrators monitor the collected data and generates patients report.
- Step 3: The received report is analysed by the doctors who then recommend the required treatment.
- Step 4: Doctors may choose to share the treatment reports using distributed database for further analysis.
- Step 5: The validated report is shared in encrypted format.
- Step 6: Patients request the Cloud Service Provider (CSP) to access their treatment record.
- Step 7: After successful validation, the encrypted file of the treatment record is received by the patient.

- Step 8: Patients decrypt the received encrypted file with their own private key in order to access their original treatment record.

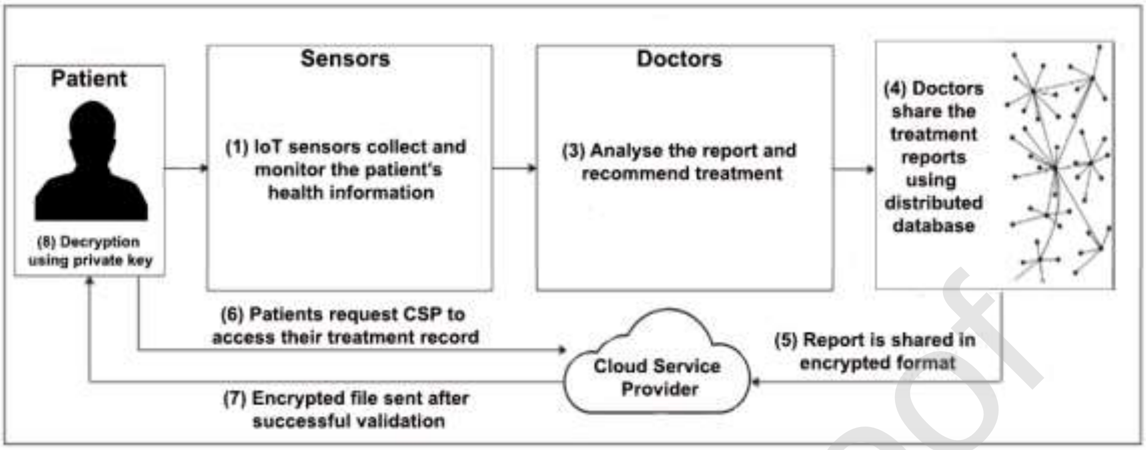


Figure 7: Blockchain for securing healthcare networks

The following sections summarize the related research on blockchain based healthcare solutions.

5.1.1 Record Management

Record management in healthcare network includes collecting as well as managing the patient's information, digital health records and medical treatment data. Mettler et al. [160] proposed a blockchain-based health bank that lends immutable, decentralized and distributed ledger properties to the healthcare networks. The work mainly focussed on user-oriented research towards public healthcare management in the medical sectors. The results obtained suggested that decentralization in healthcare networks can be achieved using blockchain technology. Zhang et al. [161] proposed a Decentralized Application (DApp) in accordance with the Health Insurance Portability and Accountability Act (HIPAA) for guaranteeing transparent, secure and anonymous transactions in a healthcare system.

5.1.2 Data Sharing and Storage

Owing to its data intensive nature, the traditional healthcare system requires to share patient's medical data among various healthcare service providers. Furthermore, securely storing the medical data and preserving its integrity in such systems is a challenging task. Yue et al. [162] proposed a blockchain based Healthcare Data Gateway (HDG) application aimed to control data sharing and provide regulatory and legal provisions in a healthcare system. Zhang et al. [163] proposed a blockchain based healthcare system that facilitates secure data sharing among nodes in a Pervasive Social Network (PSN). The proposed system consisted of a PSN area that utilize blockchain for health data sharing and a WBAN area dedicated to establish secure links. Similarly, Wang et al. [164] proposed a Parallel Healthcare System (PHS) framework for comprehensive data sharing, care auditability and medical records review. The proposed system has been tested on artificial as well as real healthcare systems in order to evaluate the effectiveness of treatment and accuracy of diagnosis. Li et al. [165] proposed EdgeCare, a secure data management scheme for mobile healthcare systems that is assisted by edge computing. Optimal incentive mechanism between users and data collector is achieved using Stackelberg game-based optimization technique. Ismail et al. [166] proposed a lightweight blockchain architecture that divide the network participants into demographic clusters in order to mitigate the communication and computational overhead associated with healthcare data management. The proposed system avoids forking problem with the help of Head BlockChain Manager (HBCM) responsible for generating blocks and handling transactions.

Table 6 presents the relative comparison of various research on blockchain based healthcare solutions.

Table 6: Comparison of blockchain based healthcare solutions

Reference	**Year**	**Blockchain Platform (Consensus used)**	**Contributions**	**Advantages**	**Shortcomings**
Mettler et al. [160]	2016	Ethereum, Bitcoin	Focussed on user-oriented research in counterfeiting the drug and public healthcare management	Tamper proof data audit and secure data access	Limited interoperability and scalability
Zhang et al. [161]	2017	Ethereum, Bitcoin, Litecoin	DApp for guaranteeing transparent, secure, anonymous and consensus-based transactions in healthcare systems.	Solves the issues of scalability and interoperability	Does not guarantee data availability and distant access
Yue et al. [162]	2016	Hyperledger Fabric	Healthcare Data Gateway (HDG) to	Guarantees security and	Do not consider the incentive

			provide regulatory and legal provisions in a healthcare system	immutability of the personal medical data	mechanism and consensus algorithm
Zhang et al. [163]	2016	Ethereum	Consisted of a PSN area (to utilize blockchain for health data sharing) and WBAN area (to establish secure links.	Guarantees identity management and secure data access	Does not provide tamper proof data audit and secure data access.
Wang et al. [164]	2018	Consortium blockchain such as Hyperledger	PHS framework for comprehensive data sharing and care auditability.	Facilitates accurate forecasting and guidance of disease treatment	Vulnerability to issues data of integrity and scalability
Li et al. [165]	2019	-	An edge computing assisted secure data management scheme for mobile healthcare systems	Reliable data protection and efficient data trading	Does not consider issues of scalability and data availability
Ismail et al. [166]	2019	Bitcoin (PBFT)	Divides the network participants into demographic clusters	Results in reduced computational overhead and avoids forking problem.	Real implementation of the architecture and its performance evaluation is yet to be done.

5.2 Smart Transportation

Smart vehicles have gained enormous attention in the past few years majorly due to the advancement of ICT. Smart transportation aims to enhance vehicle road safety, improve travel efficiency, and provide convenience to passengers as well as drivers. Blockchain technology can improve information sharing, ease vehicle communication and enhance the robustness of the overall system. Furthermore, blockchain improves the transport industry by providing reduced processing time, faster customs clearance, approvals and coordination of documents. Bernardini et al. [167] suggested that blockchain technology can effectively handle the security and privacy issues related to the Intelligent Transportation System (ITS). The proposed work provided efficient data processing, reliable data fusion, privacy preserving services and network monitoring. In another work, Sharma et al. [168] outlined the benefits of using blockchain technology for ITS in terms of improved efficiency, cost mitigation and secured service delivery to the end users. The following section summarize the related research on blockchain based smart transportation solutions.

5.2.1 Electric Vehicles (EVs)

EVs have gained increased attention in the recent past owing to the need for development of green transportation systems in many countries. EVs are battery powered and possess a communication infrastructure that facilitates information sharing among various peers. They need to pay a certain amount of money to the charging stations that are generally located in urban areas in order to ensure normal recharging of these EVs. Smart contracts and blockchain technology ease such electricity trading between charging stations and the EVs.

Knirsch et al. [169] proposed a four-stage protocol (exploration, bidding, evaluation and charging) for EV charging that enables automated, privacy preserving and reliable selection of charging stations on the basis of pricing and distance to the EV. Kang et al. [170] proposed consortium blockchain based improved electricity trading among vehicles. A shared ledger records the electricity transaction information and an iterative double action approach is adopted to optimize the electricity prices and the amount of electricity traded. Similarly, Huang et al. [171] proposed a Lightning Network and Smart Contract (LNSC) which can easily be integrated with the existing schemes to secure trading between charging piles and EVs. Kang et al. [172] proposed a two-stage security solution to defend against voting collusion between candidates in the Internet of Vehicles (IoV). The first stage is the miner selection stage that uses reputation-based voting scheme and the second stage is the block verification phase that is dedicated to prevent internal collusion between standby miners and the active miner. Zhou et al. [173] proposed a consortium based secured energy trading framework that uses contract theory-based incentive mechanism to incentivise more EVs to participate in the Demand Response (DR). In this work, authors developed a new DR framework for IoV, which leverages computational intelligence, contract threat modelling and blockchain to ensure efficient and secure energy trading.

5.2.2 Vehicular Adhoc NETworks (VANETs)

VANET is one of the most emerging technology, wherein the vehicles can communicate with the roadside unit or with each other without involvement of any central authority. However, in such autonomous environment, the adversaries might inject misleading or false information in order to exploit personal benefits. Therefore, there is a need for vehicle authentication in order to guarantee secure data exchange between these vehicles. Several researchers deployed blockchain technology for securing message transmission in VANETs.

Lei et al. [174] proposed a blockchain based system to simplify the distributed key management in heterogeneous ITS. The proposed system eliminates the central manager or the third-party authority and the key transfer mechanisms are authenticated by a decentralized Security Managers (SMs). In another work, Yang et al. [175] proposed a blockchain based decentralized trust management scheme for VANETs. Each vehicle initially rates the neighbouring vehicles and uploads the rating to the Road Side Units (RSUs). Each RSUs then estimates the trust values of these vehicles and packs them into a block using PoS and PoW consensus mechanisms. Li et al. [176] proposed CreditCoin, a blockchain based incentive vehicular announcement network that guarantees the reliability of announcements. Similarly, Gao et al. [177] proposed a privacy preserving payment scheme that secures sensitive user information and enables data sharing. Lu et al. [178] proposed a Blockchain-based Privacy Preserving Authentication (BPPA) scheme that permanently records all transactions and certificates in the blockchain. Authors extend the conventional blockchain structure by utilizing the Merkle Patricia Tree (MPT) in order to provide distributed authentication without revocation lists. Luo et al. [179] proposed a trust based blockchain enabled location privacy preserving scheme for VANETs. In this work, Dirichlet distribution-based trust management scheme is devised such that both the co-operator and the requester will only cooperate with the trusted vehicles. The trustworthiness of the vehicles is recorded on a publicly available block such that any vehicle can access the related trust information of counterparties. Feng et al. [180] introduced Blockchain-based Privacy preserving Authentication Scheme (BPAS) to provide authentication and preserve vehicle privacy in VANETs.

Table 7 presents the relative comparison of various research on blockchain based smart transportation solutions.

Table 7: Comparison of blockchain based smart transportation solutions

Reference	Year	Blockchain Platform (Consensus used)	Contributions	Advantages	Shortcomings
Knirsch et al. [169]	2017	Bitcoin	Blockchain based four-stage protocol for charging EVs.	Information related to bids of the charging stations can be stored in verifiable and transparent manner.	The proposed scheme is not scalable enough to handle high transaction volume.
Kang et al. [170]	2017	Bitcoin (PoW)	Consortium blockchain based improved electricity trading among vehicles	The amount of electricity traded among vehicles and electricity prices are effectively optimized using an iterative double auction approach.	Scalability of the proposed system is not investigated.
Huang et al. [171]	2018	Smart contract (Proof-of-Authentication)	LNSC to secure trading between charging piles and EVs.	Can be easily integrated with the existing scheduling mechanisms to enhance vehicle security	Selecting appropriate scheduling strategy is a matter of concern.
Kang et al. [172]	2019	PoW and PoS	Two stage security enhancement solution.	Defends against voting collusion between candidates in the Internet of Vehicles (IoVs).	Limited accuracy in terms of miner's reputation calculation.

Zhou et al. [173]	2019	Consortium blockchain	Consortium based secured energy trading framework	Enhanced security and performance efficiency	Incurs huge computational resource wastage which prevents the wide adoption of the proposed scheme.
Lei et al. [174]	2017	Bitcoin (PoW and PoB)	A blockchain-based secured key management scheme	The key transfer time is reduced due to effective optimization of the transaction collection period	Privacy and sustainability issue of the proposed system is not investigated.
Yang et al. [175]	2019	PoW and PoS	A blockchain-based decentralized trust management system	All RSUs collaboratively maintains a consistent and reliable public ledger.	Did not discuss the trade-off between privacy preservation and trust management
Li et al. [176]	2018	Bitcoin	A blockchain-based incentive vehicular announcement network	Guarantees reliability of the vehicular announcements.	Susceptible to issues of scalability.
Gao et al. [177]	2018	Hyperledger Fabric (Proof-of-Concept)	A blockchain-based privacy preserving payment scheme	Guarantees reliability and user authentication.	Does not preserve data integrity and data confidentiality.

Lu et al. [178]	2019	Hyperledger Fabric	BPPA scheme to preserve identity of vehicles in VANETs.	Low computation overhead to authenticate messages and identities.	Cannot provide authentication in real-time driving scenarios.
Luo et al. [179]	2020	-	A trust based blockchain enabled location privacy preserving scheme in VANET	Resilient to various trust models and is capable of preserving vehicles location privacy effectively.	Scalability of the proposed system is not yet investigated.
Feng et al. [180]	2020	Hyperledger Fabric	BPAS for VANETs that guarantees verification of the transmitted messages without the need of any centralized authority.	The proposed design is efficient, scalable and allows revocation of misbehaving vehicles.	Does not support batch verification of message groups.

5.3 Smart grid

Majority of electricity energy generated worldwide is derived from fossil fuels (e.g., oil, natural gas and coal). As over utilization of fossil energy may lead to increased greenhouse gas emission and environmental pollution, there is a need to use renewable energy. With the advents in battery energy storage technology, users tend to become prosumers by generating and storing their own electricity energy from other renewal energy [181, 182]. P2P based energy trading is a powerful perspective in smart grid where energy is exchanged between customers and the service provider. As digital transactions are performed during this energy trading process, numerous security models have been proposed to secure these transactions and protect customer's identity. In this regard, smart grid is proposed that provides secure, economical, efficient and sustainable power grid system. Apart from promoting the realization of a reliable, effective and trusted decentralized power grid system, blockchain also improves the data security and stability of these systems [183, 184]. The following sections summarize the related research on blockchain based smart grid solutions.

5.3.1 Energy Trading

Aitzhan et al. [185] proposed Priwatt, a token-based decentralized energy trading framework that can enable peers to perform energy trading in a secure manner and negotiate energy prices by leveraging multi-signature approach and blockchain technology. In another work, Gao et al. [186] proposed a blockchain enabled trust-based system to create trusted environment between the network participants. The proposed system aims to prevent the tampering of meter readings by the third party in a smart grid network. Similarly, Aggarwal et al. [187] proposed EnergyChain, a secured blockchain model that operates in three phases: (i) miner selection, (ii) block creation and validation, and (iii) energy trading. Similarly, Sheikh et al. [188] applied blockchain for energy trading between Distributed Network (DN) and EVs in order to enhance the transparency of the system and eliminate the need for any untrusted intermediary. The proposed system used a byzantine based consensus algorithm for the block verification process thereby enhancing the overall system security. In another work, Liu et al. [189] utilized private blockchain to verify transaction records among EVs. In order to achieve secure and trustful electricity trading, the proposed model relies on private blockchain based P2P electricity trading model.

5.3.2 Dynamic Pricing

Dynamic pricing in smart grids provide real-time and flexible pricing options to the consumer based on consumption profiles and the availability. In the past few years, various dynamic pricing schemes have been proposed that requires the data to travel over an insecure channel. In such scenario, adversaries might gain control over some authentic entity and cause loss to the smart grid by updating the price profiles. Blockchain has emerged as a powerful technology to guarantee reliable and secure platform for an energy internet ecosystem. Rottondi et al. [190] proposed a public blockchain based smart metering framework that utilized Shamir Secret Sharing (SSS) protocol to enable the team members to compare their overall consumption with other team members without revealing their individual data. The proposed framework also helps to guarantee data correctness and authenticity. In another work, Mengelkamp et al. [191] proposed a robust and scalable Brooklyn microgrid framework that ensures a proper balance of energy consumption and energy generation. In order to establish an efficient microgrid energy framework, authors derived seven different market components namely microgrids setup, information system, grid connection, energy management trading system, pricing mechanism, market mechanism and regulation. Similarly, Agung et al. [192] utilized blockchain to manage transactions and ensure its execution between consumers and generators in an immutable manner. The blockchain restricts the record to be modified or erased thereby preserving its immutability. Further, the proposed system also provides certainty that the customer receives electricity from the producer every time the payment is done.

Table 8 presents the relative comparison of various blockchain based smart grid solutions.

Table 8: Comparison of blockchain based smart grid solutions

Reference	Year	Blockchain Platform (Consensus used)	Contributions	Advantages	Shortcomings
Aitzhan et al. [185]	2018	Bitcoin (Proof-of-Concept)	Leverage multi-signature approach and blockchain technology to secure transactions.	Ensure identity privacy and secures transactions.	Does not solve the replication problems associated with large transaction ledgers.
Gao et al. [186]	2018	-	A blockchain enabled system to protect consumer data.	Opearations within the grid systems are automatically monitored by smart contracts.	The prototype of the systems in not yet implemented.
Aggarwal et al. [187]	2018	Bitcoin, EnergyChain (PoW)	A secured blockchain model that efficiently stores the data generated by the smart meter.	Guarantees data integrity, confidentiality and secure auditing.	Does not guarantee data malleability and data immutability.
Sheikh et al. [188]	2020	EnergyChain (PoW)	Byzantine based consensus framework to enhance the data security of energy trading processes	Enhances the overall system security and eliminates the need	The proposed system evaluated limited physical constraints of the DN and EVs.

			between DN and EVs.	for any untrusted intermediary.	
Liu et al. [189]	2019	Ethereum (PoA)	A private blockchain to verify transactions among EVs.	Ensures secure and trustful electricity trading among EVs.	Does not investigate the scalability of the proposed system.
Rottondi et al. [190]	2017	Bitcoin	A smart metering architecture that utilized Shamir Secret Sharing (SSS) protocol	Guarantee data correctness and authenticity.	Does not guarantee data auditing and confidentiality.
Mengelkamp et al. [191]	2018	Tendermint	Uses Brooklyn microgrid framework that ensures a proper balance of energy consumption and generation.	Ensures data integrity and provides efficient information sharing.	The Brooklyn Microgrid design in not fully evaluated.
Agung et al. [192]	2020	Ethereum (PoW)	Utilized blockchain to manage transactions and ensure its execution between consumers and the generator in an immutable manner.	Immutability and traceability of the transactions are preserved.	Not capable of prohibiting people from selling electricity generated from cheap or dirty energy.

5.4 Supply Chain Management (SCM)

Set of entities such as organizations and individuals that are directly involved in the flow of services, information and products, between the source and customers constitute a supply chain [193]. Across the globe, such complex supply chains have enabled manufacture and sale of numerous products, but the entities (e.g., retailers, distributors, transporters and suppliers) in these chains possess very limited knowledge about the product lifecycle. However, such product information is necessary as the *consumers* require these to enhance their trust, and *entities* require these to make business decisions or predict market trends. Therefore, the premiere requirement in a supply chain management is data sharing which can be achieved by the recent advances in blockchain technology [194 – 196]. Apart from this, blockchain can also be used to track the detailed product information, prevent entry of forged products in the market and share information among various entities in order to optimize the decision-making process.

Toyoda et al. [197] proposed a Product Ownership Management System (POMS) that enables the customer to identify forged products. In the proposed system, the possession information related to the product is tracked efficiently using blockchain. The "possession of products" is realized by implementing two smart contracts, Products Manager (PM) and Manufacturers Manager (MM). PM is responsible for tracking the position information of the products whereas MM tracks the information of the manufacturers. In another work, Wu et al. [198] proposed crowd-validated, independent, online shipment tracking framework that comprise of a single blockchain public ledger and a set of private distributed ledgers. The private ledger serves to store sensitive shipment related information and record custody events. Similarly, Sharma et al. [199] proposed a blockchain-based distributed framework in order to provide on-demand, personalized and integrated services for the automotive industry. The employed miner selection algorithm greatly enhances collaboration and communication among various participants within the supply chain. Longo et al. [200] designed a software connector to connect enterprise information systems with the blockchain so as to allow companies to share their data with varied visibility levels and build trust. The proposed system addresses the associated trust issues in a supply chain, mitigates the negative consequences of information asymmetry and discourage companies from any misconduct (e.g., low data accuracy or counterfeiting data). in another work, Salah et al. [201] leveraged smart contracts and Ethereum blockchain for soybean traceability and tracking across agricultural supply chains. All transactions are stored in the blockchains ledger and are linked to a decentralized file system to provide the desired level of traceability. In another work, Wang et al. [202] proposed a blockchain based information management scheme to address the poor traceability and fragmentation issues in a precast supply chain. Apart from guaranteeing on-time delivery, the proposed framework also facilitates tracking the cause of disputes centered on Precast Components (PCs). **Table 9** presents the relative comparison of various research on blockchain based solutions for SCM.

Table 9: Comparison of blockchain based solutions for SCM

Reference	Year	Blockchain Platform (Consensus used)	Contributions	Advantages	Shortcomings
Toyoda et al. [197]	2017	Ethereum (Proof-of-concept)	A blockchain based framework for tracking the product information.	POMS enable customers to identify forged products.	A centralized administrator is required to manage the manufacturers information.
Wu et al. [198]	2017	Proof-of-Validity	An online shipment tracking framework that comprise of a single blockchain public ledger and a set of private distributed ledgers.	Exploit benefits of both public and private ledger.	Does not discuss the time complexity associated with the public ledger.
Sharma et al. [199]	2019	Ethereum (Proof-of-concept)	A blockchain-based distributed framework to guarantee on-demand services for the automotive industry in smart cities.	Enables suppliers and manufacturers to protect their goods from fake products thereby providing feasible solution for a sustainable automotive ecosystem.	Not suitable for large organizations having numerous distributed ledgers.

Longo et al. [200]	2019	Ethereum, UnicalCoin	Software connector services that enables companies to validate the invariability, integrity and authenticity of the data shared by other companies.	Prevent companies from sending inaccurate or counterfeit data	Does not consider scalability of the proposed system.
Salah et al. [201]	2019	Ethereum	Blockchain for soybean traceability and tracking across the agricultural supply chain.	Guarantees security, integrity and reliability.	Did not address the problems of scalability, identity registrations, governance and regulations.
Wang et al. [202]	2020	Hyperledger Fabric	A blockchain based information management scheme to address poor traceability and fragmentation issues.	Enhances efficiency and information sharing among different stakeholders in a supply chain.	Working model is not yet tested.

5.5 Financial Systems

A conventional financial system is characterized by exchange of funds between the customers, investors, lenders and borrowers. Therefore, preserving privacy of the customer and maintaining security of the transaction data are the two most premier challenge. To this end, blockchain is the best proposed solution that can guarantee secure transaction management within a financial system. The transaction flow within a typical blockchain based financial system is depicted in **Figure 8** and the steps involved therein are listed as below.

- Step 1: Agreement application is sent by Alice (the payer) to the issuing bank (Bank A).
- Step 2: The issuing bank forwards the application letter to the negotiating bank (Bank B).
- Step 3: The negotiating bank sends an advising letter to Bob (the payee) requesting him to submit the confirmation documents so as to finalize the agreement.
- Step 4: Bob sends the document to Bank B.
- Step 5: Bank B forwards the received document to Bank A.
- Step 6: Bank A releases these documents to Alice who can use them to initiate a smart contract with Bob.
- Step 7-10: Secure transaction between Alice and Bob is initiated using blockchain.

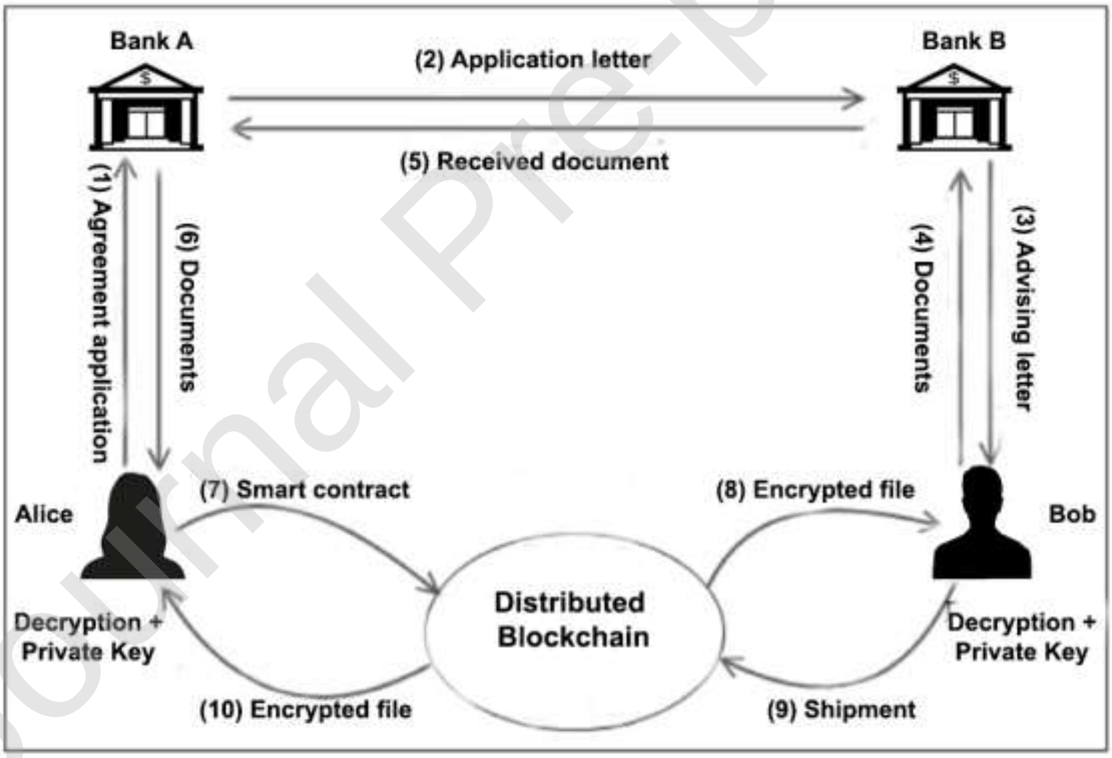


Figure 8: Blockchain in financial systems

Chen et al. [203] proposed a Bitcoin Payment Collection Supervision System (BPCSS) that saves all the transaction details on the cloud database in a cost-effective manner to help the government agencies, business enterprises and customers. In another work, Khan et al. [204] proposed a distributed ledger based global platform called Corda dedicated to record and manage the financial agreements. The proposed scheme provides reliability, scalability, risk reduction and mutualization within financial transactions. Similarly, Mccallig et al. [205] proposed to enhance financial reporting information in terms of representational faithfulness by developing an accounting information system. The proposed system provides better audit evidence to auditors for supporting their opinion and at the same time provides credible information to the stakeholders. Further, the proposed system incurs reduced agency costs between auditors and the stakeholders. Similarly, Kabra et al. [206] proposed an automated cheque clearance framework named MudraChain that uses blockchain instead of Cheque Truncation System (CTS) for effectively handling the clearance operations. The proposed framework integrates multi-level authentication scheme (to guarantee secure and tamper-proof blockchain based framework), a Quick Response (QR) generation technique (to perform digital cheque signing) and a two-factor authentication protocol (for secure funds transfer). In another work, Gao et al. [207] efficiently predicted the yield rate of blockchain based financial systems by solving the problems associated with traditional algorithms such as poor fitting effect and large number of iterations. The proposed work adopted back propagation neural network, particle swarm optimization (PSO) and Support Vector Regression (SVR) algorithm to achieve better fitting effect on yield rate predictions in blockchain financial products. **Table 10** presents the relative comparison of various research on blockchain based solutions for financial systems.

Table 10: Comparison of blockchain based solutions for financial systems

Reference	**Year**	**Blockchain Platform (Consensus used)**	**Contributions**	**Advantages**	**Shortcomings**
Chen et al. [203]	2017	Bitcoin	BPCSS to enable secure transaction between merchandise stores and customers. It is an android and java-based application.	Enhances transparency, reliability and cost effectiveness.	Does not consider identity management and fraud detection.
Khan et al. [204]	2017	Bitcoin, Corda	Corda platform dedicated to record and manage the financial	Guarantees immutability, reliability and	Does not consider data availability

			agreements. It relies on hash trees and smart contract.	data transparency in the financial systems.	and fraud detection.
Mccallig et al. [205]	2019	Bitcoin	Integrates distributed storage with network analysis and multiparty computation to enhance the representational faithfulness within financial systems.	Reduces the agency cost and enhances the transparency of the financial reporting system.	The prototype of the systems in not yet implemented and a working system is not built.
Kabra et al. [206]	2020	MudraChain (PoA)	Integrates multi-level authentication scheme, a QR generation technique and a two-factor authentication protocol.	Allows continuous flow of clearance operation without involving any intermediaries.	Does not provide real-time solution to the customers.
Gao et al. [207]	2020	Bitcoin	Adopted back propagation neural network, PSO and SVR algorithm to achieve enhanced fitting effect on yield rate prediction.	Provides better predictive effect on blockchain based financial systems.	The real-world implementation is not yet available.

5.6 Data Center Networks

Bunch of resources (including network, storage and computational resources) are interconnected via connection networks to form a data center. The network having all these data center resources is referred to as Data Center Networks (DCN). In recent years, DCNs has emerged to support huge range of services offered through e-commerce, web hosting and social networking. In a centralized infrastructure, DCN provides numerous large-scale computing and diversified network services such as cloud computing and video streaming to the subscribed users [208, 209]. The blockchain technology is being actively adopted to provide solution to privacy management, secure storage and data integrity issues of a DCN. The following subsections summarize the related research on blockchain based solutions for DCNs.

5.6.1 Cloud computing

Cloud Computing is the leading ICT-based technology that guarantees on-demand services to the end-users by creating multiple copies of the virtual resource. The data centers hosting such services consume enormous amount of energy in order to carry out their routine activity such as online data analytics and data storage. Therefore, adopting energy efficient schemes in cloud computing brings numerous benefits such as reduction in operational cost and energy consumption. Chaudhary et al. [210] proposed a Lattice-based Secure Cryptosystem for securing healthcare in future smart cities. The proposed system employs a lattice-based authentication scheme (for request validation between the cloud storage and end users), a lightweight key exchange enabled data encryption technique (for secure data exchange) and right verification mechanism (for restricting the permission grants to the end-users). Banerjee et al. [211] proposed LinkShare that relies on automated audit and access-control mechanisms to enforce data privacy. The proposed system integrates blockchain technology with the data privacy ontology to create a decentralized, trusted, auditable and secure data privacy management framework. LinkShare is able to withstand malicious attacks as it is not susceptible to single point of failure. In another work, Yang et al. [212] proposed blockchain enabled publicly verifiable data deletion technique capable of detecting malicious behaviour of the cloud server. Wang et al. [213] proposed a consortium blockchain based Electronic Health Record (EHR) sharing protocol to realize privacy preservation, data security and access control. The proposed system guarantees system availability by designing Proof of Authentication (PoA) consensus mechanism. In another work, Zhu et al. [214] proposed a Controllable Blockchain Data Management (CBDM) scheme aimed to mitigate the adverse effect of various attacks and lack of control in a blockchain network. The proposed model identifies a particular node as the Trust Authority (TA) and configures it with veto power to prevent malicious voting. Similarly, Wilczynski et al. [215] proposed a blockchain based generic cloud scheduler model aimed to offload the blockchain implementation modules and improve efficiency of the prepared schedules. The proposed model uses a novel Proof-of-Schedule (PoS) algorithm and iterative Stakelberg game to ensure secure task processing and execution.

5.6.2 Edge/Fog computing

Cloud computing systems can be optimized by edge/fog computing that relies on shifting its services, applications and data towards the end users (away from the central node). Edge computing technique serves to mitigate computational costs and improve latency by sharing the burden of increased dependency on the end users [216, 217]. However, the core challenge of security and privacy still needs to be resolved in such distributed networks. To this end, several researchers proposed blockchain based solutions to secure distributed systems.

Xiong et al. [218] proposed a mobile chain enabled edge computing framework based on optimal pricing strategy for managing distributed resources. A two-stage Stackelberg game is adopted to jointly maximize the profit of the Edge computing Service Provider (ESP) and miner utilities. The proposed framework relies on two different pricing schemes namely uniform pricing (all miners are assigned with fixed price) and discriminatory pricing (different miners are assigned with varying price). The simulation result shows that discriminatory pricing is better for meeting service demands and uniform pricing is better for maximizing profit. In another work, Jiao et al. [219] proposed an auction-based edge computing scheme aimed to maintain individual rationality and truthfulness. Similarly, Yin et al. [220] proposed HyperNet, a trusted framework to provide data privacy and sovereignty in edge computing systems. Tuli et al. [221] proposed a lightweight framework named FogBus that integrates Cloud, Fog and Edge infrastructures to support compute intensive IoT applications. The proposed framework utilizes blockchain to secure sensitive data and facilitate platform independent application execution. In another work, Memon et al. [222] proposed blockchain enabled DualFog-IoT framework aimed to decrease the system drop rate and thereby offload the cloud datacentre. Similarly, Guo et al. [223] proposed a blockchain and edge computing based trusted system aimed to improve authentication efficiency. The proposed system uses an optimized PBFT consensus algorithm to achieve activity traceability and guarantee trusted authentication. Further, the hit ratio of the system is improved using edge computing-based caching strategy. **Table 11** presents the relative comparison of various research on blockchain based solutions for DCNs.

Table 11: Comparison of blockchain based solutions for DCNs

Reference	Year	Blockchain Platform (Consensus used)	Contributions	Advantages	Shortcomings
Chaudhary et al. [210]	2018	-	A Lattice-based Secure Cryptosystem for securing healthcare systems.	Incurs low communication and computation costs.	Does not consider the issues of privacy management and data integrity.
Banerjee et al. [211]	2017	Hyperledger	LinkShare to enforce data privacy.	Guarantees confidentiality, integrity, immutability and identity management.	Does not consider scalability aspect.
Yang et al. [212]	2018	Bitcoin (PoW)	A blockchain enabled publicly verifiable data detection technique	Detects malicious behaviour of the cloud server.	Does not consider the issues of data confidentiality, data integrity and data immutability.
Wang et al. [213]	2019	Ethereum (Proof-of-Authentication)	Consortium blockchain based privacy preserving EHRs protocol realised by searchable encryption and	Preserves privacy, provides access control and guarantees systems availability.	Does not consider the issues of non-repudiation and scalability.

			proxy re-encryption.		
Zhu et al. [214]	2019	-	A controllable blockchain to address the issues of security and enhance control on the posted ledgers.	Minimizes distributive storage waste and enhances block construction efficiency.	The prototype is yet to be implemented in real-world environment.
Wilczynski et al. [215]	2020	Proof-of-Schedule (PoSch)	A blockchain based generic cloud scheduler model that uses a novel PoSch algorithm and iterative Stakelberg game	Ensures secure processing and execution of tasks as per end user requirements.	Suitability for multi cloud systems is yet to be tested.
Jiao et al. [219]	2018	Ethereum	Uses Vickrey Clarke Groves mechanism, Greedy approach and S-shape utility function.	Maintains individual rationality and enhances truthfulness.	Did not consider the aspects of scalability, data immutability and interoperability.
Yin et al. [220]	2018	-	Uses keyless signature infrastructure and smart contract.	Provides data sovereignty and identity management.	Does not guarantee data confidentiality, immutability and availability.
Tuli et al. [221]	2019	-	A FogBus framework that	Proposed framework is secure, scalable,	Does not support dynamic resource

			facilitates IoT application deployment, management and resource sharing.	cost efficient and easy to deploy.	management and runtime application migration.
Memon et al. [222]	2019	Ethereum	DualFog-IoT architecture that inherits the features of blockchain to achieve security and privacy.	Incurs reduced operational expenses and energy resource expenditure.	Does not consider data availability and fraud detection.
Guo et al. [223]	2020	PBFT	A blockchain and edge computing based trusted system.	Guarantees trusted authentication and achieves activity traceability	Needs further optimization in terms of availability and performance.

6. Open Issues and Future Research Directions

The notion of smart city is still evolving and the requirements of maturity and robustness in blockchain based smart city solutions make it an extremely fluid and fats-moving area. Therefore, prior to its widespread implementation, numerous significant research challenges need to be addressed in the near future. As part of the survey, the following section outlines various challenges and future research directions.

6.1 Intelligent Participatory Sensing for Smart Cities

Communities and individuals use cloud services and mobile phones to collect and analyse data in participatory sensing in order to provide information about the environmental parameters [224, 225]. This enables various smart city applications (such as energy controlling and health-care) to compare the collected online data with the available data. However, the existing smart city infrastructure is incapable of using these features. Further, there is a need to design a new framework that exploits participatory sensing to collect data from trusted authorities and perform real time analysis.

6.2 Security and Privacy

The smart city comprises of a plethora of interconnected devices. Therefore, it becomes necessary for the security solutions to centre around a system of defence rather than providing individual defences. Therefore, transparent privacy standards and layered security approaches becomes crucial for a smart city [226, 227]. The major challenge in blockchain based smart city systems is maintaining security and privacy. The root cause of privacy issues in a blockchain network is that users in such network remains pseudonymous rather than being completely anonymous. Owing to the transparent nature of blockchain technology, the transactions are publicly available and visible for all network participants [228, 229]. This might lead to tracking of user activities and revealing the real-world identity of the participants. Such information can be exploited to gain access to financial secrets (e.g., spending pattern, income and wealth). Therefore, there is a need to ensure true anonymity.

6.3 Storage

Owing to the explosive rise in the amount of data being generated by smart city devices, managing and storing these data is prominent challenge. Several researches have labelled cloud storage to be the most appropriate approach in this regard as the cloud servers possess immense storage capacity and computing resources [230, 231]. However, storing the data on the cloud is unreliable and inefficient in smart city applications because uploading of data to the cloud servers might cause long delays or even compromise the data integrity. Furthermore, the malicious behaviour or the untrusted nature of the cloud service providers makes it necessary for the data owners to verify the integrity of the outsourced data. To this end, several centralized data storage schemes have been proposed. However, these schemes are vulnerable to single point of failure and DoS attack. In order to overcome such issues, blockchain based decentralized storage schemes have been proposed. Kopp et al. [232] proposed a decentralized token system named 'Koppercoin' that uses proof of retrievability (PoR) instead of PoW. This approach requires the participants to contribute file storage and earn digital tokens in the process thereby providing direct reward to contributing participants. Ruj et al. [233] proposed a blockchain based secured decentralized storage framework named 'BlockStore' aimed to ensure higher transparency, enhanced security and faster audits. BlockStrore maintains a record of un-utilized storage within the space wallet and assigns them on rent. Even though, the decentralized systems overcome the limitations of the centralized storage systems, it still faces some issues such as lack of trust, lack of privacy and security, etc. Furthermore, in traditional blockchain systems, each node must possess the capability to process and maintain complete transactions back to the genesis block. Therefore, applying blockchain technology to such resource constrained smart city is a challenge and requires further investigation.

6.4 Energy Efficiency

Energy efficiency needs to be considered seriously due to the rapidly rising energy costs in smart cities [234, 235]. Several consensus schemes such as PoW are computationally expensive as the network nodes need to perform complex computations in order to mine the next block. Owing to such complex and redundant computations in PoW, it incurs huge electricity energy consumption and is therefore not considered as an energy efficient approach [236, 237]. To this end, researchers developed comparatively less computationally expensive consensus mechanisms such as PoS, DPoS [62] and PBFT [72]. However, the BFT based schemes lack scalability and thus are not suited for large scale systems. A new consensus protocol named proof of trust [92] is proposed that addresses the issues of throughput, scalability, security and energy consumption by leveraging a trust model. Despite being highly promising, these consensus mechanism needs further investigation as PBFT lacks scalability and the security of PoS is not yet rigorously investigated. Therefore, there is a need to investigate energy efficient consensus scheme for blockchain based smart city systems.

6.5 Scalability and Performance

Blockchain based solutions in a smart city must meet demand of business and government-based sectors, especially regarding scalability and performance. In this regard, several researchers focussed on increasing the number of replicas. But this also increases the number of messages beings exchanged which brings forth several performance concerns such as latency (time taken to append a block to the blockchain) and throughput (number of successful transactions per second) [238]. Even though, PoW consensus mechanism enhances scalability, it suffers from problems of high latency and low throughput especially due to the wastage of resources in solving cryptographically difficult puzzle. Furthermore, PoW is CPU intensive and susceptible to double spending attack [239]. This results in lengthy transaction duration making it unfit for real-time applications. PBFT protocol achieves consensus even in presence of malicious replicas and is energy efficient but lacks scalability. Any mainstream platform must be capable of processing thousands of transactions per second in order to keep the economy of the smart city moving without any significant delay. Therefore, scalability and performance of blockchain based smart city solution is an important concern and needs further investigation.

6.6 Incentive Mechanism

Nodes in smart cities are assumed to be self-interested and therefore incentive mechanisms (such as transaction fees and currency issuance) are needed to motivate these nodes to contribute towards data verification. In scenarios where group of nodes collectively generate blocks, it is important to design an incentive mechanism to allocate transaction fees to the deserving nodes [240]. On the other hand, it also important to design a punishment mechanism to punish malicious nodes and prevent double spending attacks. Recently, several works have been proposed in this regard. Wu et al. [241] proposed an incentive platform aimed to enhance the participating detectors for vulnerability detection thereby enabling customers to receive automatic security feedback. In another work, Weng et al. [242] proposed a secure, distributed framework that employs value-driven incentive scheme to force the network participants to behave genuinely. The proposed scheme provides auditability as well as guarantees data privacy. Similarly, Wang et al. [243] proposed a reputation-based scheme that encourage both malicious and normal nodes to participate in the network operations. The proposed scheme aims to reward the cooperative nodes and punish the non-cooperative ones. However, because of several reasons, none of these solutions are universally accepted. Therefore, designing an effective incentive and punishment mechanism needs further investigation.

6.7 Interoperability

The design of blockchain technology standards is not yet universally accepted. Several bodies such as NIST and IEEE are in the process of designing standards for blockchain integration, governance and interoperability [244, 245]. Implementing an interoperable system is a challenging task due to wide range of data formats involved in various blockchain systems [246]. This complexity is further increased due to dissimilar consensus mechanisms adopted by autonomous blockchain systems. For example, Hyperledger uses PBFT, and Ethereum uses PoW consensus mechanism, and in order to enable seamless operation, these two mechanisms need to be synchronized. Therefore, it is necessary to transmit data from one blockchain to another in order to facilitate seamless application development platform. Thus, designing interoperable protocols for blockchain-based smart city solutions needs further investigation.

6.8 Regulation

The decentralized blockchain platforms tend to weaken the ability of central banks to dominate the economic policy. Therefore, the government becomes prudent towards the use of cryptocurrencies and the blockchain platforms face regularity issues [247]. Many countries including Morocco, Iran and Pakistan banned the use of cryptocurrencies in their territories. Yeoh et al. [248] highlighted the major regulatory issues that have adverse impact on blockchains and innovative distributed technologies, especially in the USA and the European Union (EU) [248]. Therefore, new industry and government regulations are needed in order to evade disputes among the transacting parties as there is no need for a trusted intermediary for a decentralized blockchain technology. Furthermore, various smart city devices generate data in different unstructured data formats. Directly storing these heterogeneous and unstructured data in the blockchain based systems in not an effective approach. In order to enable seamless data exchange among various entities of a smart city, careful consideration of storage standards and data formats is required [249]. Therefore, regulation rules for ensuring data integrity in blockchain based smart city systems is an open research challenge.

7. Conclusion

The explosive growth in the world's population coupled with the rapid urbanisation process tend to endanger the environmental and economical sustainability of cities. To this end, the concept of "Smart City" is proposed that use modern ICT in an intelligent manner so as to build a sustainable urban environment and improve the citizens life. However, there are proliferating security challenges in smart cities. These challenges can be effectively addressed by the use of blockchain technology, owing to its good properties such as auditability, transparency, immutability and decentralization. In this paper, the possibilities and benefits of applying blockchain technology to smart cities along with its trade-offs are presented through a comprehensive survey. The paper begins with some related recently published surveys and background knowledge of blockchain and smart cities. Then, the motivation behind applying blockchain technology to the realm of smart cities is discussed. Further, the paper aims to integrate the two areas by exploring and critically reviewing the utility of blockchain in various smart communities such as healthcare, transportation, smart grid, supply chain management, financial systems and data center networks. Finally, numerous open challenges are outlined for future research directions in related areas. This survey is expected to serve as a knowledge base and systematic guideline for future research in applying blockchain technology to smart cities.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] United Nations, "Population Division," Dec. 2017. [Online]. Available: http://www.un.org/en/development/desa/population/
[2] "World urbanization prospects: The 2014 revision, highlights (ST/ESA/SER.A/352)," United Nations, Department of Economic and Social Affairs, Population Division, Tech. Rep., 2014. [Online]. Available: https://esa.un.org/unpd/wup/Publications/Files/WUP2014- Highlights.pdf
[3] Malik, K. R., Sam, Y., Hussain, M., & Abuarqoub, A. (2018). A methodology for real-time data sustainability in smart city: Towards inferencing and analytics for big-data. *Sustainable Cities and Society, 39,* 548-556. DOI: 10.1016/j.scs.2017.11.031
[4] Bibri, S. E., & Krogstie, J. (2017). Smart sustainable cities of the future: An extensive interdisciplinary literature review. *Sustainable Cities and Society, 31,* 183-212. DOI: 10.1016/j.scs.2017.02.016
[5] Collotta, M., & Pau, G. (2017). An Innovative Approach for Forecasting of Energy Requirements to Improve a Smart Home Management System Based on BLE. *IEEE Transactions on Green Communications and Networking, 1*(1), 112-120. DOI: 10.1109/tgcn.2017.2671407
[6] Amin, S. U., Hossain, M. S., Muhammad, G., Alhussein, M., & Rahman, M. A. (2019). Cognitive Smart Healthcare for Pathology Detection and Monitoring. *IEEE Access, 7,* 10745-10753. DOI: 10.1109/access.2019.2891390
[7] Pramanik, P. K., Pareek, G., & Nayyar, A. (2019). Security and Privacy in Remote Healthcare. *Telemedicine Technologies,* 201-225. DOI: 10.1016/b978-0-12-816948-3.00014-3
[8] Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. (2018). BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. *2018 IEEE Globecom Workshops (GC Wkshps).* DOI: 10.1109/glocomw.2018.8644088
[9] Ridhawi, I. A., Otoum, S., Aloqaily, M., Jararweh, Y., & Baker, T. (2020). Providing secure and reliable communication for next generation networks in smart cities. *Sustainable Cities and Society, 56,* 102080. DOI: 10.1016/j.scs.2020.102080
[10] Alotaibi, S. S. (2019). Registration Center Based User Authentication Scheme for Smart E-Governance Applications in Smart Cities. *IEEE Access, 7,* 5819-5833. DOI: 10.1109/access.2018.2884541
[11] Mohammad, N. (2019). A Multi-Tiered Defense Model for the Security Analysis of Critical Facilities in Smart Cities. *IEEE Access, 7,* 152585-152598. DOI: 10.1109/access.2019.2947638
[12] Shen, M., Tang, X., Zhu, L., Du, X., & Guizani, M. (2019). Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT Data in Smart Cities. *IEEE Internet of Things Journal, 6*(5), 7702–7712. DOI: 10.1109/jiot.2019.2901840
[13] Deep, G., Mohana, R., Nayyar, A., Sanjeevikumar, P., & Hossain, E. (2019). Authentication Protocol for Cloud Databases Using Blockchain Mechanism. *Sensors, 19*(20), 4444. DOI:10.3390/s19204444
[14] S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.
[15] Wang, T., Zheng, Z., Rehmani, M. H., Yao, S., & Huo, Z. (2019). Privacy Preservation in Big Data From the Communication Perspective—A Survey. *IEEE Communications Surveys & Tutorials, 21*(1), 753–778. DOI: 10.1109/comst.2018.2865107
[16] Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195. DOI: 10.1109/jiot.2018.2812239
[17] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials, 18*(3), 2084-2123. DOI: 10.1109/comst.2016.2535718
[18] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4,* 2292-2303. DOI: 10.1109/access.2016.2566339
[19] Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J., & Ko, K. (2018). Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access, 6,* 1513-1524. DOI: 10.1109/access.2017.2779263
[20] Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks, 141,* 199-221. DOI: 10.1016/j.comnet.2018.03.012
[21] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88,* 173-190. DOI: 10.1016/j.future.2018.05.046

[22] Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2019). Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys & Tutorials, 21*(1), 858-880. DOI: 10.1109/comst.2018.2863956
[23] Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys & Tutorials, 21*(3), 2794-2830. DOI: 10.1109/comst.2019.2899617
[24] Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet of Things Journal, 6*(2), 2188-2204. DOI: 10.1109/jiot.2018.2882794
[25] Syed, T. A., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., & Alghamdi, T. (2019). A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. *IEEE Access, 7*, 176838-176869. DOI: 10.1109/access.2019.2957660
[26] Sookhak, M., Tang, H., He, Y., & Yu, F. R. (2019). Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges. *IEEE Communications Surveys & Tutorials, 21*(2), 1718-1743. DOI: 10.1109/comst.2018.2867288
[27] Aggarwal, S., Chaudhary, R., Aujla, G. S., Kumar, N., Choo, K. R., & Zomaya, A. Y. (2019). Blockchain for smart communities: Applications, challenges and opportunities. *Journal of Network and Computer Applications, 144*, 13-48. DOI: 10.1016/j.jnca.2019.06.018
[28] Sengupta, J., Ruj, S., & Bit, S. D. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of Network and Computer Applications, 149*, 102481. DOI: 10.1016/j.jnca.2019.102481
[29] Moniruzzaman, M., Khezr, S., Yassine, A., & Benlamri, R. (2020). Blockchain for smart homes: Review of current trends and research challenges. *Computers & Electrical Engineering, 83*, 106585. DOI: 10.1016/j.compeleceng.2020.106585
[30] Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society, 55*, 102018. DOI: 10.1016/j.scs.2020.102018
[31] Abdullah, S., Rothenberg, S., Siegel, E., & Kim, W. (2020). School of Block–Review of Blockchain for the Radiologists. *Academic Radiology*, *27*(1), 47–57. DOI: 10.1016/j.acra.2019.06.025
[32] Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. *Internet of Things*, *8*, 100107. DOI: 10.1016/j.iot.2019.100107
[33] Arora, D., Gautham, S., Gupta, H., & Bhushan, B. (2019). Blockchain-based Security Solutions to Preserve Data Privacy and Integrity. *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. DOI: 10.1109/icccis48478.2019.8974503
[34] Decker, C., & Wattenhofer, R. (2013). Information propagation in the Bitcoin network. *IEEE P2P 2013 Proceedings*. DOI: 10.1109/p2p.2013.6688704
[35] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, *30*(7), 1366–1385. DOI: 10.1109/tkde.2017.2781227
[36] Saini, H., Bhushan, B., Arora, A., & Kaur, A. (2019). Security vulnerabilities in Information communication technology: Blockchain to the rescue (A survey on Blockchain Technology). *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. DOI: 10.1109/icicict46008.2019.8993229
[37] Maesa, D. D. F., & Mori, P. (2020). Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing*, *138*, 99–114. DOI: 10.1016/j.jpdc.2019.12.019
[38] Yuan, Y., & Wang, F.-Y. (2018). Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *48*(9), 1421–1428. DOI: 10.1109/tsmc.2018.2854904
[39] Manimuthu, A., V., R. S., G., R., & Marwaha, D. (2019). A Literature Review on Bitcoin: Transformation of Crypto Currency Into a Global Phenomenon. *IEEE Engineering Management Review*, *47*(1), 28–35. DOI: 10.1109/emr.2019.2901431
[40] Delgado-Segura, S., Pérez-Solà, C., Navarro-Arribas, G., & Herrera-Joancomartí, J. (2019). Analysis of the Bitcoin UTXO Set. *Financial Cryptography and Data Security Lecture Notes in Computer Science*, 78–91. DOI: 10.1007/978-3-662-58820-8_6
[41] Douceur, J. R. (2002). The Sybil Attack. *Peer-to-Peer Systems Lecture Notes in Computer Science*, 251–260. DOI: 10.1007/3-540-45748-8_24
[42] Yang, C., Chen, X., & Xiang, Y. (2018). Blockchain-based publicly verifiable data deletion scheme for cloud storage. *Journal of Network and Computer Applications*, *103*, 185–193. DOI: 10.1016/j.jnca.2017.11.011
[43] Chen, H., & Wang, Y. (2019). SSChain: A full sharding protocol for public blockchain without data migration overhead. *Pervasive and Mobile Computing*, *59*, 101055. DOI: 10.1016/j.pmcj.2019.101055

[44] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. *IEEE Consumer Electronics Magazine*, *7*(4), 6–14. DOI: 10.1109/mce.2018.2816299
[45] M. Castro, B. Liskov et al., "Practical byzantine fault tolerance," in OSDI, vol. 99, 1999, pp. 173–186.
[46] G. Sachs, "Blockchain–putting theory into practice," the-blockchain. com, pp. 25–32, 2016.
[47] Huang, X., Zhang, Y., Li, D., & Han, L. (2019). An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains. *Future Generation Computer Systems*, *91*, 555–562. DOI: 10.1016/j.future.2018.09.046
[48] Wang, Q., Zhao, H., Wang, Q., Cao, H., Aujla, G. S., & Zhu, H. (2019). Enabling secure wireless multimedia resource pricing using consortium blockchains. *Future Generation Computer Systems*. DOI: 10.1016/j.future.2019.09.026
[49] Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401. DOI: 10.1145/357172.357176
[50] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., … Kim, D. I. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access*, *7*, 22328–22370. DOI: 10.1109/access.2019.2896108
[51] Memon, R., Li, J., & Ahmed, J. (2019). Simulation Model for Blockchain Systems Using Queuing Theory. *Electronics*, *8*(2), 234. DOI: 10.3390/electronics8020234
[52] Saleh, F. (2018). Blockchain Without Waste: Proof-of-Stake. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.3183935
[53] Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. *Advances in Cryptology – CRYPTO 2017 Lecture Notes in Computer Science*, 357–388. DOI: 10.1007/978-3-319-63688-7_12
[54] Li, W., Andreina, S., Bohli, J.-M., & Karame, G. (2017). Securing Proof-of-Stake Blockchain Protocols. *Lecture Notes in Computer Science Data Privacy Management, Cryptocurrencies and Blockchain Technology*, 297–315. DOI: 10.1007/978-3-319-67816-0_17
[55] V. Buterin and V. Griffith, "Casper the friendly finality gadget," arXiv preprint arXiv:1710.09437, 2017.
[56] King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.
[57] P. Vasin, "Blackcoins proof-of-stake protocol v2," URL: https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf, vol. 71, 2014.
[58] Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34–37. DOI: 10.1145/2695533.2695545
[59] Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*, *195*, 234–246. DOI: 10.1016/j.apenergy.2017.03.039
[60] S. Wilkinson, J. Lowry, and T. Boshevski, "Metadisk a blockchain based decentralized file storage application," Storj Labs Inc., Technical Report, hal, pp. 1–11, 2014.
[61] Bozic, N., Pujolle, G., & Secci, S. (2016). A tutorial on blockchain and applications to secure network control-planes. *2016 3rd Smart Cloud Networks & Systems (SCNS)*. DOI: 10.1109/scns.2016.7870552
[62] D. Larimer, "Delegated proof-of-stake (dpos)," Bitshare whitepaper, 2014.
[63] "Delegated proof-of-stake consensus — bitshares 3.0," https://bitshares.org/technology/delegated-proof-of-stake-consensus/ (Accessed on 05/05/2020).
[64] Intel: Sawtooth Lake (2017). https://intelledger.github.io/
[65] Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On Security Analysis of Proof-of-Elapsed-Time (PoET). *Lecture Notes in Computer Science Stabilization, Safety, and Security of Distributed Systems*, 282–297. DOI: 10.1007/978-3-319-69084-1_19
[66] Wang, X., Weili, J., & Chai, J. (2018). The Research on the Incentive Method of Consortium Blockchain Based on Practical Byzantine Fault Tolerant. *2018 11th International Symposium on Computational Intelligence and Design (ISCID)*. DOI: 10.1109/iscid.2018.10136
[67] Su, L., & Vaidya, N. H. (2017). Reaching approximate Byzantine consensus with multi-hop communication. *Information and Computation*, *255*, 352–368. DOI: 10.1016/j.ic.2016.12.003
[68] Gramoli, V. (2017). From blockchain consensus back to Byzantine consensus. *Future Generation Computer Systems*. DOI: 10.1016/j.future.2017.09.023
[69] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," Stellar Development Foundation, 2015.
[70] Nasreen, M., Ganesh, A., & Sunitha, C. (2016). A Study on Byzantine Fault Tolerance Methods in Distributed Networks. *Procedia Computer Science*, *87*, 50–54. DOI: 10.1016/j.procs.2016.05.125
[71] Rakitin, S., Visheratin, A. A., & Nasonov, D. (2018). Byzantine fault-tolerant and semantic-driven consensus protocol. *Procedia Computer Science*, *136*, 25–34. DOI: 10.1016/j.procs.2018.08.234

[72] De Angelis, Stefano, Aniello, Leonardo, Baldoni, Roberto, Lombardi, Federico, Margheri, Andrea and Sassone, Vladimiro (2018) PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain. *Italian Conference on Cyber Security.* 11 pp .
[73] Su, L., & Vaidya, N. H. (2017). Reaching approximate Byzantine consensus with multi-hop communication. *Information and Computation, 255*, 352–368. DOI: 10.1016/j.ic.2016.12.003
[74] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone. Blockchain-based database to ensure data integrity in cloud computing environments. In ITA-SEC, volume 1816. CEUR-WS.org, 2017.
[75] Aura. https://github.com/paritytech/parity/wiki/Aura.
[76] Clique. https://github.com/ethereum/EIPs/issues/225.
[77] Dib, Omar, Kei-Leo Brousmiche, Antoine Durand, Eric Thea, and E. Ben Hamida, (2018) "Consortium blockchains: Overview, applications and challenges", International Journal On Advances in Telecommunications 11, no. 1&2.
[78] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. DOI: 10.1109/smc.2017.8123011
[79] Ongaro, Diego, and John Ousterhout, (2014), "In search of an understandable consensus algorithm." In 2014 USENIX Annual Technical Conference (USENIXATC 14), pp. 305-319.
[80] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.
[81] Singh, S. K., Rathore, S., & Park, J. H. (2019). BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. *Future Generation Computer Systems*. DOI: 10.1016/j.future.2019.09.002
[82] Venkatesh, V., Kang, K., Wang, B., Zhong, R. Y., & Zhang, A. (2020). System architecture for blockchain based transparency of supply chain social sustainability. *Robotics and Computer-Integrated Manufacturing, 63*, 101896. DOI: 10.1016/j.rcim.2019.101896
[83] Yu, F. R., Liu, J., He, Y., Si, P., & Zhang, Y. (2018). Virtualization for Distributed Ledger Technology (vDLT). *IEEE Access, 6*, 25019–25028. DOI: 10.1109/access.2018.2829141
[84] Wang, X., Li, L., Yuan, Y., Ye, P., & Wang, F. (2016). ACP-based social computing and parallel intelligence: Societies 5.0 and beyond. *CAAI Transactions on Intelligence Technology, 1*(4), 377-393. DOI: 10.1016/j.trit.2016.11.005
[85] Wang, X., Zheng, X., Zhang, X., Zeng, K., & Wang, F. (2017). Analysis of Cyber Interactive Behaviors Using Artificial Community and Computational Experiments. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 47*(6), 995-1006. DOI: 10.1109/tsmc.2016.2615130
[86] Neudecker, T., & Hartenstein, H. (2019). Network Layer Aspects of Permissionless Blockchains. *IEEE Communications Surveys & Tutorials, 21*(1), 838-857. DOI: 10.1109/comst.2018.2852480
[87] Yang, W., Aghasian, E., Garg, S., Herbert, D., Disiuta, L., & Kang, B. (2019). A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future. *IEEE Access, 7*, 75845-75872. DOI: 10.1109/access.2019.2917562
[88] Zhang, S., & Lee, J. (2020). A Group Signature and Authentication Scheme for Blockchain-Based Mobile-Edge Computing. *IEEE Internet of Things Journal, 7*(5), 4557-4565. DOI: 10.1109/jiot.2019.2960027
[89] Hyla, T., & Pejaś, J. (2020). Long-term verification of signatures based on a blockchain. *Computers & Electrical Engineering, 81*, 106523. DOI: 10.1016/j.compeleceng.2019.106523
[90] Lakshman, T. V., & Agrawala, A. K. (1986). Efficient decentralized consensus protocols. *IEEE Transactions on Software Engineering, SE-12*(5), 600–607. DOI: 10.1109/tse.1986.6312956
[91] Miller, A., Juels, A., Shi, E., Parno, B., & Katz, J. (2014). Permacoin: Repurposing Bitcoin Work for Data Preservation. *2014 IEEE Symposium on Security and Privacy*. DOI: 10.1109/sp.2014.37
[92] Zou, J., Ye, B., Qu, L., Wang, Y., Orgun, M. A., & Li, L. (2019). A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services. *IEEE Transactions on Services Computing, 12*(3), 429–445. DOI: 10.1109/tsc.2018.2823705
[93] Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016). Proof of Luck. *Proceedings of the 1st Workshop on System Software for Trusted Execution - SysTEX 16*. DOI: 10.1145/3007788.3007790
[94] Yuan, Y., Wang, F., & Zeng, D. (2017). Competitive Analysis of Bidding Behavior on Sponsored Search Advertising Markets. *IEEE Transactions on Computational Social Systems, 4*(3), 179-190. doi:10.1109/tcss.2017.2730925
[95] Li, J., Ni, X., & Yuan, Y. (2018). The Reserve Price of Ad Impressions in Multi-Channel Real-Time Bidding Markets. *IEEE Transactions on Computational Social Systems, 5*(2), 583-592. doi:10.1109/tcss.2018.2831234
[96] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. *2016 IEEE Symposium on Security and Privacy (SP)*. DOI: 10.1109/sp.2016.55

[97] "Solidity," June. 2018. [Online]. Available: https://solidity.readthedocs.io/en/develop/
[98] Hildenbrandt, E., Saxena, M., Rodrigues, N., Zhu, X., Daian, P., Guth, D., . . . Rosu, G. (2018). KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine. *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*. DOI: 10.1109/csf.2018.00022
[99] Wu, J., Dong, M., Ota, K., Li, J., & Yang, W. (2020). Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT. *IEEE Network*, *34*(1), 69-75. DOI: 10.1109/mnet.001.1900179
[100] Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., & Rong, C. (2019). A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond. *IEEE Internet of Things Journal*, *6*(5), 8114-8154. DOI: 10.1109/jiot.2019.2922538
[101] Nicolas, C., Kim, J., & Chi, S. (2020). Quantifying the dynamic effects of smart city development enablers using structural equation modeling. *Sustainable Cities and Society*, *53*, 101916. DOI: 10.1016/j.scs.2019.101916
[102] Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, *55*, 102023. DOI: 10.1016/j.scs.2020.102023
[103] Rathore, M. M., Paul, A., Hong, W., Seo, H., Awan, I., & Saeed, S. (2018). Exploiting IoT and big data analytics: Defining Smart Digital City using real-time urban data. *Sustainable Cities and Society*, *40*, 600-610. DOI: 10.1016/j.scs.2017.12.022
[104] Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, *50*, 101660. DOI: 10.1016/j.scs.2019.101660
[105] Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society*, *39*, 499–507. DOI: 10.1016/j.scs.2018.02.039
[106] Singh, A., Sharma, A., Sharma, N., Kaushik, I., & Bhushan, B. (2019). Taxonomy of Attacks on Web Based Applications. *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. DOI: 10.1109/icicict46008.2019.8993264
[107] Varshney, T., Sharma, N., Kaushik, I., & Bhushan, B. (2019). Architectural Model of Security Threats & their Countermeasures in IoT. *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. DOI: 10.1109/icccis48478.2019.8974544
[108] Arora, A., Kaur, A., Bhushan, B., & Saini, H. (2019). Security Concerns and Future Trends of Internet of Things. *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. DOI: 10.1109/icicict46008.2019.8993222
[109] Bhushan, B., & Sahoo, G. (2017). Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. *Wireless Personal Communications*,*98*(2), 2037-2077. DOI: 10.1007/s11277-017-4962-0
[110] Wu, J., Ota, K., Dong, M., & Li, C. (2016). A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities. *IEEE Access*, *4*, 416–424. DOI: 10.1109/access.2016.2517321
[111] Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine*, *5*(3), 60–70. DOI: 10.1109/mce.2016.2556879
[112] Jong, M. D., Joss, S., Schraven, D., Zhan, C., & Weijnen, M. (2015). Sustainable–smart–resilient–low carbon–eco–knowledge cities; making sense of a multitude of concepts promoting sustainable urbanization. *Journal of Cleaner Production*, *109*, 25–38. DOI: 10.1016/j.jclepro.2015.02.004
[113] Oakley, D., & Tsao, H.-S. (2007). Socioeconomic gains and spillover effects of geographically targeted initiatives to combat economic distress: An examination of Chicago's Empowerment Zone. *Cities*, *24*(1), 43–59. DOI: 10.1016/j.cities.2006.10.003
[114] Sasaki, M. (2010). Urban regeneration through cultural creativity and social inclusion: Rethinking creative city theory through a Japanese case study. *Cities*, *27*. DOI: 10.1016/j.cities.2010.03.002
[115] Datta, A. (2015). New urban utopias of postcolonial India. *Dialogues in Human Geography*, *5*(1), 3–22. DOI: 10.1177/2043820614565748
[116] Caragliu, A., Bo, C. D., & Nijkamp, P. (2011). Smart Cities in Europe. *Journal of Urban Technology*, *18*(2), 65–82. DOI: 10.1080/10630732.2011.601117
[117] Shi, X., & Li, X. (2018). Research on three-stage dynamic relationship between carbon emission and urbanization rate in different city groups. *Ecological Indicators*, *91*, 195–202. DOI: 10.1016/j.ecolind.2018.03.056
[118] Silva, B. N., Khan, M., & Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society*, *38*, 697–713. DOI: 10.1016/j.scs.2018.01.053

[119] Sun, R., Lü, Y., Yang, X., & Chen, L. (2019). Understanding the variability of urban heat islands from local background climate and urbanization. *Journal of Cleaner Production, 208,* 743–752. DOI: 10.1016/j.jclepro.2018.10.178
[120] Kitchin, R. (2013). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1–14. DOI: 10.1007/s10708-013-9516-8
[121] Nam, T., & Pardo, T. A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. *Proceedings of the 12th Annual International Digital Government Research Conference on Digital Government Innovation in Challenging Times - Dg.o 11*. DOI: 10.1145/2037556.2037602
[122] Lombardi, P., Giordano, S., Farouh, H., & Yousef, W. (2012). Modelling the smart city performance. *Innovation: The European Journal of Social Science Research*, *25*(2), 137–149. DOI: 10.1080/13511610.2012.660325
[123] Bhushan, B., & Sahoo, G. (2017). A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks. *2017 International Conference on Signal Processing and Communication (ICSPC)*. DOI: 10.1109/cspc.2017.8305856
[124] Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. *2017 International Conference on Signal Processing and Communication (ICSPC)*. DOI: 10.1109/cspc.2017.8305855
[125] Li, N., Liu, D., & Nepal, S. (2017). Lightweight Mutual Authentication for IoT and Its Applications. *IEEE Transactions on Sustainable Computing, 2*(4), 359-370. DOI: 10.1109/tsusc.2017.2716953
[126] Mick, T., Tourani, R., & Misra, S. (2018). LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities. *IEEE Internet of Things Journal, 5*(2), 755-764. DOI: 10.1109/jiot.2017.2725238
[127] Mahmood, K., Chaudhry, S. A., Naqvi, H., Kumari, S., Li, X., & Sangaiah, A. K. (2018). An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems, 81*, 557-565. DOI: 10.1016/j.future.2017.05.002
[128] Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2020). Lightweight elliptic curve cryptography accelerator for internet of things applications. *Ad Hoc Networks, 103*, 102159. DOI: 10.1016/j.adhoc.2020.102159
[129] Hammi, B., Fayad, A., Khatoun, R., Zeadally, S., & Begriche, Y. (2020). A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT). *IEEE Systems Journal*, 1-11. DOI: 10.1109/jsyst.2020.2970167
[130] Luo, X., Yin, L., Li, C., Wang, C., Fang, F., Zhu, C., & Tian, Z. (2020). A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment. *IEEE Access, 8*, 67192-67204. DOI: 10.1109/access.2020.2978525
[131] Zhang, P., Liu, J., Shen, Y., Li, H., & Jiang, X. (2020). Lightweight Tag-Based PHY-Layer Authentication for IoT Devices in Smart Cities. *IEEE Internet of Things Journal, 7*(5), 3977-3990. DOI: 10.1109/jiot.2019.2958079
[132] "Cisco security monitoring, analysis and response system." [Online]. Available: https://www.cisco.com/c/en/us/products/security/securitymonitoring-analysis-response-system/index.html
[133] Kaps, J., Yuksel, K., & Sunar, B. (2005). Energy Scalable Universal Hashing. *IEEE Transactions on Computers*, *54*(12), 1484–1495. DOI: 10.1109/tc.2005.195
[134] Sinaeepourfard, A., Garcia, J., Masip-Bruin, X., & Marin-Tordera, E. (2017). A Novel Architecture for Efficient Fog to Cloud Data Management in Smart Cities. *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. DOI: 10.1109/icdcs.2017.202
[135] Saeed, F., Paul, A., Rehman, A., Hong, W., & Seo, H. (2018). IoT-Based Intelligent Modeling of Smart Home Environment for Fire Prevention and Safety. *Journal of Sensor and Actuator Networks*, *7*(1), 11. DOI: 10.3390/jsan7010011
[136] Alohali, B. (2016). Security in Cloud of Things (CoT). *Advances in Systems Analysis, Software Engineering, and High Performance Computing Managing Big Data in Cloud Computing Environments*, 46–70. DOI: 10.4018/978-1-4666-9834-5.ch003
[137] Wen, H., Tang, J., Wu, J., Song, H., Wu, T., Wu, B., … Sun, L.-M. (2015). A Cross-Layer Secure Communication Model Based on Discrete Fractional Fourier Fransform (DFRFT). *IEEE Transactions on Emerging Topics in Computing*, *3*(1), 119–126. DOI: 10.1109/tetc.2014.2367415
[138] Shamir, A. (1985). Identity-Based Cryptosystems and Signature Schemes. *Advances in Cryptology Lecture Notes in Computer Science*, 47–53. DOI: 10.1007/3-540-39568-7_5
[139] Sandhu, R., Coyne, E., Feinstein, H., & Youman, C. (1996). Role-based access control models. *Computer*, *29*(2), 38–47. DOI: 10.1109/2.485845
[140] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security - CCS 06*. DOI: 10.1145/1180405.1180418

[141] Sookhak, M., Yu, F. R., Khan, M. K., Xiang, Y., & Buyya, R. (2017). Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. *Future Generation Computer Systems*, *72*, 273–287. DOI: 10.1016/j.future.2016.08.018
[142] Lanza, J., Sánchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., & Gutiérrez, V. (2015). Large-Scale Mobile Sensing Enabled Internet-of-Things Testbed for Smart City Services. *International Journal of Distributed Sensor Networks, 11*(8), 785061. DOI: 10.1155/2015/785061
[143] "Santander Facility," June. 2018. [Online]. Available: http://www.smartsantander.eu/index.php/testbeds/item/132santander-summary
[144] Latre, S., Leroux, P., Coenen, T., Braem, B., Ballon, P., & Demeester, P. (2016). City of things: An integrated and multi-technology testbed for IoT smart city experiments. *2016 IEEE International Smart Cities Conference (ISC2)*. DOI: 10.1109/isc2.2016.7580875
[145] "Smart City Testbed NYUAD," June. 2018. [Online]. Available: http://sites.nyuad.nyu.edu/ccs-ad/about/research-areas-2/researchlabs-groups/smart-city-testbed/
[146] Cardone, G., Cirri, A., Corradi, A., & Foschini, L. (2014). The participact mobile crowd sensing living lab: The testbed for smart cities. *IEEE Communications Magazine*, *52*(10), 78–85. DOI: 10.1109/mcom.2014.6917406
[147] Soni, S., & Bhushan, B. (2019). A Comprehensive survey on Blockchain: Working, security analysis, privacy threats and potential applications. *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. DOI: 10.1109/icicict46008.2019.8993210
[148] Gupta, S., Sinha, S., & Bhushan, B. (2020). Emergence of Blockchain Technology: Fundamentals, Working and its Various Implementations. *SSRN Electronic Journal*. DOI:10.2139/ssrn.3569577
[149] Madaan, L., Kumar, A., & Bhushan, B. (2020). Working principle, Application areas and Challenges for Blockchain Technology. *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*. DOI: 10.1109/csnt48778.2020.9115794
[150] Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, *86*, 650–655. DOI: 10.1016/j.future.2018.04.060
[151] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297. DOI: 10.1016/j.scs.2018.02.014
[152] Li, Z., Bahramirad, S., Paaso, A., Yan, M., & Shahidehpour, M. (2019). Blockchain for decentralized transactive energy management system in networked microgrids. *The Electricity Journal*, *32*(4), 58–72. DOI: 10.1016/j.tej.2019.03.008
[153] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing*, *134*, 180–197. DOI: 10.1016/j.jpdc.2019.08.005
[154] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407. DOI: 10.1016/j.jisa.2019.102407
[155] López, D., & Farooq, B. (2020). A multi-layered blockchain framework for smart mobility data-markets. *Transportation Research Part C: Emerging Technologies*, *111*, 588–615. DOI: 10.1016/j.trc.2020.01.002
[156] Sun, M., & Zhang, J. (2020). Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. *Computer Communications*, *149*, 332–342. DOI: 10.1016/j.comcom.2019.10.031
[157] Chaudhary, R., Jindal, A., Aujla, G. S., Kumar, N., Das, A. K., & Saxena, N. (2018). LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. *IEEE Communications Magazine*, *56*(4), 24–32. DOI: 10.1109/mcom.2018.1700787
[158] Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220. DOI: 10.1093/jamia/ocx068
[159] Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. P. C. (2018). BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. *2018 IEEE Globecom Workshops (GC Wkshps)*. DOI: 10.1109/glocomw.2018.8644088
[160] Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*. DOI: 10.1109/healthcom.2016.7749510
[161] Zhang, P., Liu, Z., Han, S., He, L., Müller, H. S., Zhao, T., & Wang, Y. (2017). Visualization of rapid penetration of water into cracked cement mortar using neutron radiography. *Materials Letters*, *195*, 1–4. DOI: 10.1016/j.matlet.2017.02.077

[162] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *Journal of Medical Systems*, *40*(10). DOI: 10.1007/s10916-016-0574-6
[163] Zhang, J., Xue, N., & Huang, X. (2016). A Secure System For Pervasive Social Network-Based Healthcare. *IEEE Access*, *4*, 9239–9250. DOI: 10.1109/access.2016.2645904
[164] Wang, S., Wang, J., Wang, X., Qiu, T., Yuan, Y., Ouyang, L., … Wang, F.-Y. (2018). Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *IEEE Transactions on Computational Social Systems*, *5*(4), 942–950. DOI: 10.1109/tcss.2018.2865526
[165] Li, X., Huang, X., Li, C., Yu, R., & Shu, L. (2019). EdgeCare: Leveraging Edge Computing for Collaborative Data Management in Mobile Healthcare Systems. *IEEE Access*, *7*, 22011–22025. DOI: 10.1109/access.2019.2898265
[166] Ismail, L., Materwala, H., & Zeadally, S. (2019). Lightweight Blockchain for Healthcare. *IEEE Access*, *7*, 149935–149951. DOI: 10.1109/access.2019.2947613
[167] Bernardini, C., Asghar, M. R., & Crispo, B. (2017). Security and privacy in vehicular communications: Challenges and opportunities. *Vehicular Communications*, *10*, 13–28. DOI: 10.1016/j.vehcom.2017.10.002
[168] Sharma, P. K., Chen, M.-Y., & Park, J. H. (2018). A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access*, *6*, 115–124. DOI: 10.1109/access.2017.2757955
[169] Knirsch, F., Unterweger, A., & Engel, D. (2017). Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Computer Science - Research and Development*, *33*(1-2), 71–79. DOI: 10.1007/s00450-017-0348-5
[170] Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., & Hossain, E. (2017). Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. *IEEE Transactions on Industrial Informatics*, *13*(6), 3154–3164. DOI: 10.1109/tii.2017.2709784
[171] Huang, X., Xu, C., Wang, P., & Liu, H. (2018). LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. *IEEE Access*, *6*, 13565–13574. DOI: 10.1109/access.2018.2812176
[172] Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D. I., & Zhao, J. (2019). Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Transactions on Vehicular Technology*, *68*(3), 2906–2920. DOI: 10.1109/tvt.2019.2894944
[173] Zhou, Z., Wang, B., Guo, Y., & Zhang, Y. (2019). Blockchain and Computational Intelligence Inspired Incentive-Compatible Demand Response in Internet of Electric Vehicles. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *3*(3), 205–216. DOI: 10.1109/tetci.2018.2880693
[174] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Internet of Things Journal*, *4*(6), 1832–1843. DOI: 10.1109/jiot.2017.2740569
[175] Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. M. (2019). Blockchain-Based Decentralized Trust Management in Vehicular Networks. *IEEE Internet of Things Journal*, *6*(2), 1495–1505. DOI: 10.1109/jiot.2018.2836144
[176] Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., & Zhang, Z. (2018). CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *19*(7), 2204–2220. DOI: 10.1109/tits.2017.2777990
[177] Gao, F., Zhu, L., Shen, M., Sharif, K., Wan, Z., & Ren, K. (2018). A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks. *IEEE Network*, *32*(6), 184–192. DOI: 10.1109/mnet.2018.1700269
[178] Lu, Z., Wang, Q., Qu, G., Zhang, H., & Liu, Z. (2019). A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *27*(12), 2792–2801. DOI: 10.1109/tvlsi.2019.2929420
[179] Luo, B., Li, X., Weng, J., Guo, J., & Ma, J. (2020). Blockchain Enabled Trust-Based Location Privacy Protection Scheme in VANET. *IEEE Transactions on Vehicular Technology*, *69*(2), 2034–2048. DOI: 10.1109/tvt.2019.2957744
[180] Feng, Q., He, D., Zeadally, S., & Liang, K. (2020). BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. *IEEE Transactions on Industrial Informatics*, *16*(6), 4146–4155. DOI: 10.1109/tii.2019.2948053
[181] Park, S., Lee, J., Bae, S., Hwang, G., & Choi, J. K. (2016). Contribution-Based Energy-Trading Mechanism in Microgrids for Future Smart Grid: A Game Theoretic Approach. *IEEE Transactions on Industrial Electronics*, *63*(7), 4255–4265. DOI: 10.1109/tie.2016.2532842
[182] Al-Turjman, F., Altrjman, C., Din, S., & Paul, A. (2019). Energy monitoring in IoT-based ad hoc networks: An overview. *Computers & Electrical Engineering*, *76*, 133-142. DOI: 10.1016/j.compeleceng.2019.03.013

[183] Wang, S., Taha, A. F., Wang, J., Kvaternik, K., & Hahn, A. (2019). Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(8), 1612–1623. DOI: 10.1109/tsmc.2019.2916565
[184] Wang, J., Wu, L., Choo, K.-K. R., & He, D. (2020). Blockchain-Based Anonymous Authentication With Key Management for Smart Grid Edge Computing Infrastructure. *IEEE Transactions on Industrial Informatics*, *16*(3), 1984–1992. DOI: 10.1109/tii.2019.2936278
[185] Aitzhan, N. Z., & Svetinovic, D. (2018). Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Transactions on Dependable and Secure Computing*, *15*(5), 840–852. DOI: 10.1109/tdsc.2016.2616861
[186] Gao, J., Asamoah, K. O., Sifah, E. B., Smahi, A., Xia, Q., Xia, H., … Dong, G. (2018). Grid Monitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid. *IEEE Access*, *6*, 9917–9925. DOI: 10.1109/access.2018.2806303
[187] Aggarwal, S., Chaudhary, R., Aujla, G. S., Jindal, A., Dua, A., & Kumar, N. (2018). EnergyChain. *Proceedings of the 1st ACM MobiHoc Workshop on Networking and Cybersecurity for Smart Cities - SmartCitiesSecurity18*. DOI: 10.1145/3214701.3214704
[188] Sheikh, A., Kamuni, V., Urooj, A., Wagh, S., Singh, N., & Patel, D. (2020). Secured Energy Trading Using Byzantine-Based Blockchain Consensus. *IEEE Access*, *8*, 8554–8571. DOI: 10.1109/access.2019.2963325
[189] Liu, H., Zhang, Y., Zheng, S., & Li, Y. (2019). Electric Vehicle Power Trading Mechanism Based on Blockchain and Smart Contract in V2G Network. *IEEE Access*, *7*, 160546–160558. DOI: 10.1109/access.2019.2951057
[190] Rottondi, C., & Verticale, G. (2017). A Privacy-Friendly Gaming Framework in Smart Electricity and Water Grids. *IEEE Access*, *5*, 14221–14233. DOI: 10.1109/access.2017.2727552
[191] Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets. *Applied Energy*, *210*, 870–880. DOI: 10.1016/j.apenergy.2017.06.054
[192] Agung, A. A. G., & Handayani, R. (2020). Blockchain for smart grid. *Journal of King Saud University - Computer and Information Sciences*. DOI: 10.1016/j.jksuci.2020.01.002
[193] Mentzer, J. T., Dewitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining Supply Chain Management. *Journal of Business Logistics*, *22*(2), 1–25. DOI: 10.1002/j.2158-1592.2001.tb00001.x
[194] Cui, P., Dixon, J., Guin, U., & Dimase, D. (2019). A Blockchain-Based Framework for Supply Chain Provenance. *IEEE Access*, *7*, 157113–157125. DOI: 10.1109/access.2019.2949951
[195] Gonczol, P., Katsikouli, P., Herskind, L., & Dragoni, N. (2020). Blockchain Implementations and Use Cases for Supply Chains-A Survey. *IEEE Access*, *8*, 11856–11871. DOI: 10.1109/access.2020.2964880
[196] Helo, P., & Shamsuzzoha, A. (2020). Real-time supply chain—A blockchain architecture for project deliveries. *Robotics and Computer-Integrated Manufacturing*, *63*, 101909. DOI: 10.1016/j.rcim.2019.101909
[197] Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain. *IEEE Access*, *5*, 17465-17477. DOI: 10.1109/access.2017.2720760
[198] Wu, H., Li, Z., King, B., Miled, Z. B., Wassick, J., & Tazelaar, J. (2017). A Distributed Ledger for Supply Chain Physical Distribution Visibility. *Information*, *8*(4), 137. DOI: 10.3390/info8040137
[199] Sharma, P. K., Kumar, N., & Park, J. H. (2019). Blockchain-Based Distributed Framework for Automotive Industry in a Smart City. *IEEE Transactions on Industrial Informatics*, *15*(7), 4197-4205. DOI: 10.1109/tii.2018.2887101
[200] Longo, F., Nicoletti, L., Padovano, A., D'atri, G., & Forte, M. (2019). Blockchain-enabled supply chain: An experimental study. *Computers & Industrial Engineering*, *136*, 57-69. DOI: 10.1016/j.cie.2019.07.026
[201] Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain-Based Soybean Traceability in Agricultural Supply Chain. *IEEE Access*, *7*, 73295-73305. DOI: 10.1109/access.2019.2918000
[202] Wang, Z., Wang, T., Hu, H., Gong, J., Ren, X., & Xiao, Q. (2020). Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. *Automation in Construction*, *111*, 103063. DOI: 10.1016/j.autcon.2019.103063
[203] Chen, P., Jiang, B., & Wang, C. (2017). Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet. *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. DOI: 10.1109/wimob.2017.8115844
[204] Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., & Thompson, C. (2017). A Distributed-Ledger Consortium Model for Collaborative Innovation. *Computer*, *50*(9), 29-37. DOI: 10.1109/mc.2017.3571057
[205] Mccallig, J., Robb, A., & Rohde, F. (2019). Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain. *International Journal of Accounting Information Systems*, *33*, 47-58. DOI: 10.1016/j.accinf.2019.03.004

[206] Kabra, N., Bhattacharya, P., Tanwar, S., & Tyagi, S. (2020). MudraChain: Blockchain-based framework for automated cheque clearance in financial institutions. *Future Generation Computer Systems, 102*, 574-587. DOI: 10.1016/j.future.2019.08.035
[207] Gao, W., & Su, C. (2020). Analysis of earnings forecast of blockchain financial products based on particle swarm optimization. *Journal of Computational and Applied Mathematics, 372*, 112724. DOI: 10.1016/j.cam.2020.112724
[208] Aujla, G. S., Singh, M., Kumar, N., & Zomaya, A. Y. (2019). Stackelberg Game for Energy-Aware Resource Allocation to Sustain Data Centers Using RES. *IEEE Transactions on Cloud Computing, 7*(4), 1109-1123. DOI: 10.1109/tcc.2017.2715817
[209] Kumar, N., Aujla, G. S., Garg, S., Kaur, K., Ranjan, R., & Garg, S. K. (2019). Renewable Energy-Based Multi-Indexed Job Classification and Container Management Scheme for Sustainability of Cloud Data Centers. *IEEE Transactions on Industrial Informatics, 15*(5), 2947-2957. DOI: 10.1109/tii.2018.2800693
[210] Chaudhary, R., Jindal, A., Aujla, G. S., Kumar, N., Das, A. K., & Saxena, N. (2018). LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. *IEEE Communications Magazine, 56*(4), 24-32. DOI: 10.1109/mcom.2018.1700787
[211] Banerjee, A., & Joshi, K. P. (2017). Link before you share: Managing privacy policies through blockchain. *2017 IEEE International Conference on Big Data (Big Data)*. DOI: 10.1109/bigdata.2017.8258482
[212] Yang, C., Chen, X., & Xiang, Y. (2018). Blockchain-based publicly verifiable data deletion scheme for cloud storage. *Journal of Network and Computer Applications, 103*, 185-193. DOI: 10.1016/j.jnca.2017.11.011
[213] Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain. *IEEE Access, 7*, 136704-136719. DOI: 10.1109/access.2019.2943153
[214] Zhu, L., Wu, Y., Gai, K., & Choo, K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. *Future Generation Computer Systems, 91*, 527-535. DOI: 10.1016/j.future.2018.09.019
[215] Wilczyński, A., & Kołodziej, J. (2020). Modelling and simulation of security-aware task scheduling in cloud computing based on Blockchain technology. *Simulation Modelling Practice and Theory, 99*, 102038. DOI: 10.1016/j.simpat.2019.102038
[216] Garg, S., Singh, A., Kaur, K., Aujla, G. S., Batra, S., Kumar, N., & Obaidat, M. S. (2019). Edge Computing-Based Security Framework for Big Data Analytics in VANETs. *IEEE Network, 33*(2), 72-81. DOI: 10.1109/mnet.2019.1800239
[217] Aujla, G. S., Kumar, N., Garg, S., Kaur, K., & Ranjan, R. (2019). EDCSuS: Sustainable Edge Data Centers as a Service in SDN-enabled Vehicular Environment. *IEEE Transactions on Sustainable Computing*, 1-1. DOI: 10.1109/tsusc.2019.2907110
[218] Xiong, Z., Feng, S., Niyato, D., Wang, P., & Han, Z. (2018). Optimal Pricing-Based Edge Computing Resource Management in Mobile Blockchain. *2018 IEEE International Conference on Communications (ICC)*. DOI: 10.1109/icc.2018.8422517
[219] Jiao, Y., Wang, P., Niyato, D., & Xiong, Z. (2018). Social Welfare Maximization Auction in Edge Computing Resource Allocation for Mobile Blockchain. *2018 IEEE International Conference on Communications (ICC)*. DOI: 10.1109/icc.2018.8422632
[220] Yin, H., Guo, D., Wang, K., Jiang, Z., Lyu, Y., & Xing, J. (2018). Hyperconnected Network: A Decentralized Trusted Computing and Networking Paradigm. *IEEE Network, 32*(1), 112-117. DOI: 10.1109/mnet.2018.1700172
[221] Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2019). FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing. *Journal of Systems and Software, 154*, 22-36. DOI: 10.1016/j.jss.2019.04.050
[222] Memon, R. A., Li, J. P., Nazeer, M. I., Khan, A. N., & Ahmed, J. (2019). DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things. *IEEE Access, 7*, 169073-169093. DOI: 10.1109/access.2019.2952472
[223] Guo, S., Hu, X., Guo, S., Qiu, X., & Qi, F. (2020). Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System. *IEEE Transactions on Industrial Informatics, 16*(3), 1972-1983. DOI: 10.1109/tii.2019.2938001
[224] Estrin, D. (2010). Participatory sensing: Applications and architecture [Internet Predictions]. *IEEE Internet Computing, 14*(1), 12-42. DOI: 10.1109/mic.2010.12
[225] Peng, J., Zhu, Y., Zhao, Q., Zhu, H., Cao, J., Xue, G., & Li, B. (2017). Fair Energy-Efficient Sensing Task Allocation in Participatory Sensing with Smartphones. *The Computer Journal, 60*(6), 850-865. DOI: 10.1093/comjnl/bxx015
[226] Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access, 6*, 46134-46145. DOI: 10.1109/access.2018.2853985

[227] Al- Turjman, F., Zahmatkesh, H., & Shahroze, R. (2019). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*. DOI: 10.1002/ett.3677
[228] Nagel, E., & Kranz, J. (2020). Smart City Applications on the Blockchain: Development of a Multi-layer Taxonomy. *Progress in IS Blockchain and Distributed Ledger Technology Use Cases,* 201-226. DOI: 10.1007/978-3-030-44337-5_10
[229] Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (2020). Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. *IEEE Network, 34*(1), 8-14. DOI: 10.1109/mnet.001.1900178
[230] Mokhtari, G., Anvari-Moghaddam, A., & Zhang, Q. (2019). A New Layered Architecture for Future Big Data-Driven Smart Homes. *IEEE Access, 7*, 19002-19012. DOI: 10.1109/access.2019.2896403
[231] Alli, A. A., & Alam, M. M. (2019). SecOFF-FCIoT: Machine learning based secure offloading in Fog-Cloud of things for smart city applications. *Internet of Things, 7*, 100070. DOI: 10.1016/j.iot.2019.100070
[232] Kopp, H., Bösch, C., & Kargl, F. (2016). KopperCoin – A Distributed File Storage with Financial Incentives. *Information Security Practice and Experience Lecture Notes in Computer Science,* 79-93. DOI: 10.1007/978-3-319-49151-6_6
[233] Ruj, S., Rahman, M. S., Basu, A., & Kiyomoto, S. (2018). BlockStore: A Secure Decentralized Storage Framework on Blockchain. *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*. DOI: 10.1109/aina.2018.00157
[234] Kirimtat, A., Krejcar, O., Kertesz, A., & Tasgetiren, M. F. (2020). Future Trends and Current State of Smart City Concepts: A Survey. *IEEE Access, 8*, 86448-86467. DOI: 10.1109/access.2020.2992441
[235] Manchanda, C., Sharma, N., Rathi, R., Bhushan, B., & Grover, M. (2020). Neoteric Security and Privacy Sanctuary Technologies in Smart Cities. *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*. DOI: 10.1109/csnt48778.2020.9115780
[236] Conoscenti, M., Vetro, A., & Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. DOI: 10.1109/aiccsa.2016.7945805
[237] Mendling, J., Weber, I., Aalst, W. V., Brocke, J. V., Cabanillas, C., Daniel, F., . . . Zhu, L. (2018). Blockchains for Business Process Management - Challenges and Opportunities. *ACM Transactions on Management Information Systems, 9*(1), 1-16. DOI: 10.1145/3183367
[238] Vukolić, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *Open Problems in Network Security Lecture Notes in Computer Science,* 112-125. DOI: 10.1007/978-3-319-39028-4_9
[239] Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Čapkun, S. (2015). Misbehavior in Bitcoin. *ACM Transactions on Information and System Security, 18*(1), 1-32. DOI: 10.1145/2732196
[240] Fisch, B., Pass, R., & Shelat, A. (2017). Socially Optimal Mining Pools. *Web and Internet Economics Lecture Notes in Computer Science,* 205-218. DOI: 10.1007/978-3-319-71924-5_15
[241] Wu, B., Li, Q., Xu, K., Li, R., & Liu, Z. (2018). SmartRetro: Blockchain-Based Incentives for Distributed IoT Retrospective Detection. *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. DOI: 10.1109/mass.2018.00053
[242] Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., & Luo, W. (2019). DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-based Incentive. *IEEE Transactions on Dependable and Secure Computing,* 1-1. DOI: 10.1109/tdsc.2019.2952332
[243] Wang, E. K., Liang, Z., Chen, C., Kumari, S., & Khan, M. K. (2020). PoRX: A reputation incentive scheme for blockchain consensus of IIoT. *Future Generation Computer Systems, 102*, 140-151. DOI: 10.1016/j.future.2019.08.005
[244] Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain Standards for Compliance and Trust. *IEEE Cloud Computing, 4*(4), 84-90. DOI: 10.1109/mcc.2017.3791019
[245] Kakavand, H., Sevres, N. K., & Chilton, B. (2017). The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2849251
[246] Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys & Tutorials,* 1-1. DOI: 10.1109/comst.2020.2969706
[247] Kakavand, H., Sevres, N. K., & Chilton, B. (2017). The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2849251
[248] Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance, 25*(2), 196-208. DOI: 10.1108/jfrc-08-2016-0068
[249] Dewan, S., & Singh, L. (2020). Use of blockchain in designing smart city. *Smart and Sustainable Built Environment, Ahead-of-print*(Ahead-of-print). DOI: 10.1108/sasbe-06-2019-0078