International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 11, No.1 (Jan-2022)

https://dx.doi.org/10.12785/ijcds/110101

Ensuring Security and Transparency in Distributed Communication in IoT ecosystems using Blockchain Technology: Protocols, Applications and Challenges

Jahangeer Ali[1] **and Shabir A. Sofi**[2]

[1]*Department of Information Technology, National Institute of Technology, Srinagar, India*
[2]*Assistant Professor, Department of of Information Technology, National Institute of Technology, Srinagar, India*

Received 22 Jun. 2020, Revised 23 Jun. 2021, Accepted 8 Jul. 2021, Published 15 Jan. 2022

Abstract: Internet of Things (IoT) has become a widespread ubiquitous technology connecting seamlessly the physical world with the internet. The security, trust, and privacy issues are still serious challenges in IoT, as less work has been done on the security aspect. Blockchain technology seems to be the viable solution to maintain security, transparency, auditability, immutability, and privacy in a decentralized manner without any third party intermediary. The main objective of this paper is based on comparative analysis in the existing literature comprising of consensus mechanisms, smart contracts, architectures, service platforms, and application use cases in blockchain-based IoT (BIoT). This paper presents a comprehensive review and the flow of information starting from: vast IoT applications and the main challenges in its adoption, integration of blockchain with IoT and applications. Finally, some important challenges were discussed in order to have a novel network of IoT nodes having security, privacy, transparency throughout the communication medium.

Keywords: IoT, Blockchain, Consensus Mechanisms, Smart Contracts, Fog computing, BIoT Applications, Challenges

1. Introduction

A. Internet of Things (IoT)

Internet of things is the seamless interconnection of smart objects having some computational and computing capabilities to interact with the environment by collecting data and automating majority of the tasks. The IoT enabled environments have transformed the perception of dealing with physical things beyond simple data gathering tools[1]. IoT is growing at a very fast speed, IoT devices are believed to be nearly 30 billion devices by the end of 2020[2]. IoT has changed the lifestyle and interaction of humans in fact other living creatures as well. IoT has direct impact on the world economy. The IoT market revenue is increasing predicted by Cisco expecting to around 14.4 trillion between 2013 and 2022. IoT is based on integration of various standards mostly in wireless communication and enabling technologies with varying characteristics like sensing, storage, connectivity, computing and other capabilities. In order to provide seamless connectivity of everything poses a serious challenge for the implementation of IoT. In this regard various international organisations, institutes, industries and researchers have time to time carried out developments standardization and innovation but there is still need of comprehensive system with integration guidelines beneath one IoT vision [3]. With the tremendous adoption of smart objects under the banner of internet of things, covering different application areas like precision agriculture, supply chain management, logistics, smart cities, healthcare, industrial automation, disaster management systems, smart markets, smart vehicles and many in continuation [1], [4], [5], [6], [7]. IoT mostly relies on the centralized client server architectures where security, privacy is of much concern [8], [9]. These IoT devices are limited in resources which makes them vulnerable to the security treats in the shared medium [10], [11]. The IoT for large scale development is growing in majority of the areas with more challenging security provisions [4]. With the experience of rapid growth in its adoption, less importance is given to the security and privacy features because of resource-constrained nature of IoT objects [12]. Data shared by these objects contains some confidential and personal information, and thus security attacks are possible to exploit the weaknesses of present IoT infrastructures. Most of IoT infrastructures have single point of failure, which stops the wide spread adoption of IoT. IoT ecosystems manages to make the life of humans much better but the information available with the IoT devices may not

E-mail address: jehangirnit@gmail.com, shabir@nitsri.net

fit the legacy business models to the various e-businesses [13].

B. Blockchain

Blockchain comprises of a decentralized and distributed ledger that can record transactions between two or more participating nodes efficiently in a verifiable and permanent way. Blockchain consists of cryptographically chain of blocks in a tamper-proof trustless communication. Blockchain is to be considered as distributed, uncompromised and tamper resistant ledger database [14]. In blockchain network, the transactional blocks are easily accessible but no one can modify any portion of the block with confirmed submission in the chain [15]. Blockchain can be efficiently used to address the security issues of IoT, mainly data integrity and reliability. Blockchain allows applications to send and record transactions in a secured and peer to peer manner [16], [17], [18]. The distributed ledger can be applied in networks where data exchange takes place. Transaction is considered to be the basic unit of blockchain. Every time a new transaction (block) is created, it is broadcast to entire blockchain network [16]. Blockchain [19] is a database which stores all the transactional data in chronological order in the form of chained blocks without any provision to modify by the adversaries. Blockchain is an ecosystem of large parties maintaining the data integrity and providing the all transactional parties with the working proof in a decentralized manner. Blockchain is cryptographic based linked-list structure consists of blocks, where each block consists of header, meta data and transactional data linked with hashes of previous block [20], [15], [9]. The agents inside any distributed system work based on some well defined agreement rules. Likewise, in blockchain the computing nodes are working under the agreement of distributed consensus. Blockchain has a capability to provide universal accessibility, transparency, store and transfer data in a secure way throughout the network by maintaining the anonymity. Blockchain maintains the data integrity and unchanging state of the committed block stored in the distributed ledger [21], [22]. Blockchain technology comes out to be the promising solution for maintaining the data blocks captured by large number of IoT devices in order to monitor, coordinate, carry out transactions and store information in a distributed ledger and the local copy of the blockchain is maintained by peer nodes in the network enabling the creations of applications that require no centralized cloud. IBM has monitored blockchain as a technology for uniformity in the future of IoT [23].

C. Expansion of Blockchain

Blockchain (BC) has evolved tremendously since its inception by the S. Nakamoto and team in the design of virtual currency (Bitcoin). The blockchain technology started from the cryptocurrencies and further applied in majority of the systems were huge data is exchanged between the nodes [24]. The blockchain technology has moved from the virtual currency, smart contracts in financial services to IoT based applications integrated with blockchain technology which can be programmed easily [9]. The researchers are exploring the BC technology implementation footprints in most of the applications. These applications include supply chain management, logistics, healthcare, agriculture, pharmaceutics, smart-grids etc. The BC technology possesses various distinguished properties like decentralization, security, transparency, immutability and auditability. The vision of modern IoT based businesses can be achieved by integrating it with blockchain [25]. Blockchain is considered to be the ideal solution for untrusted IoT based environments by maintaining decentralization, security, transparency and immutability [2]. Blockchain technology is growing at a rapid pace from past few years. As reported by Statista [23] investments by many stake-holders in blockchain startups rose from 93 to 550 million (US dollars) from 2013 to 2016. Furthermore, the market for blockchain technology in worldwide is expected to grow 2.3 billion US dollars by 2021. The blockchain technology is considered to be better alternative for the trust and security related issues in IoT networks [26]. Gartner Inc. suggested that US firms are adopting blockchain in 75% of IoT based applications till 2020 [27]. Figure 1 highlighted the growth and expectation of various technologies, applications associated with the blockchain technology.

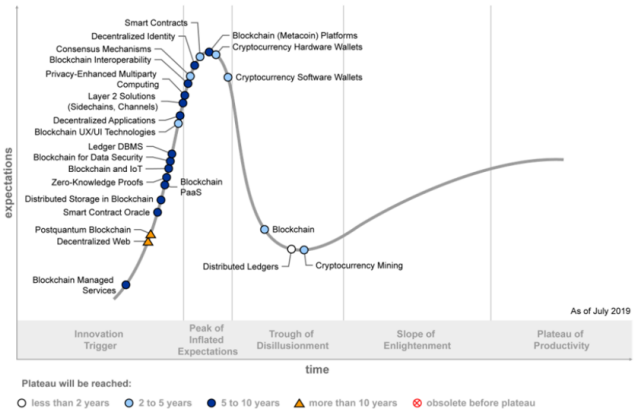

Figure 1. Hype cycle for blockchain business.

D. Building Blocks of Blockchain

Blockchain technology maintains transparency, security and accountability among the transaction records in much more better way in a distributed ledger. The basic framework of blockchain network consists of various important concepts which are discussed as following [28]:

Block: The block is the basic unit of operation in blockchain. It stores and maintains information related to transactions carried out between multiple parties in the blockchain network. Hash based cryptographic security is provided in the blockchain network in which blocks are connected to each other in chained structure by their hash codes in a distributed ledger. A simple block consists of two parts; one part comprises of header which contains metadata

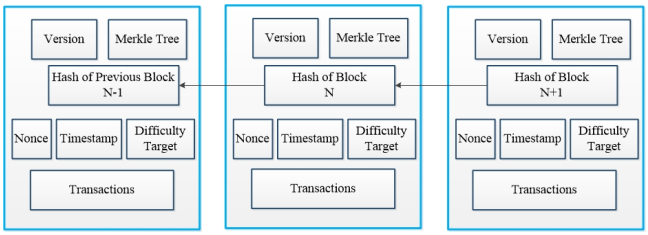

Figure 2. Structure of chained blocks in blockchain.

about the blocks in the ledger, second part contains actual data about the transactions in the blockchain network [29]. Figure 2 depicts the basic block diagram of a block used in network chained together with the block header information mentioned as under:

Version number: 4 bytes for the version number of the block.

Previous block hash: 32 bytes is used for the hash of the previous block.

Timestamp: 4 bytes to store the current time of block creation.

Merkle tree: 32 bytes which stores all the hashes and the transactions with SHA-256.

Difficulty target: 4 bytes to set the difficulty target of the block as per requirement.

Nonce: 4 bytes for the creation of block and calculate hashes for block validation.

Hash function: The blocks in the distributed ledger of blockchain are connected to each other with the hash codes. It is a complex process to solve the hash function in order to process a block. Since hash function is one way function, any small change in the input block will change the hash drastically. Blocks are identified by their hash codes maintaining identity and integrity verification [30]. The hash value of previous block is stored in the header portion of the next block thus forming the chain of blocks. The indexing mechanisms are efficient enough as the hash values are stored in the Merkle tree [31].

Miner Node: The specialized nodes that can solve the complex mathematical challenges posed by the participating parties in order to accept their blocks in the main blockchain network. The users initially broadcast the blocks in the form of transactions to all the nodes in the network. Based on the consensus algorithms implemented in the blockchain network, the miner nodes will verify the incoming block after successful attempt will add the block in the chain [30].

Transaction: It is the basic unit of work to be carried out blockchain network that is stored in distributed ledger. The transactions in the form of blocks are verified, stored and executed in the blockchain by majority of peers involved in the blockchain network. The earlier transactions can be seen at any time but cannot be modified. The miners require more power and memory space as the size of blockchain increases over the time, while smaller transactions require less and are faster in performance [30].

E. Characteristics of Blockchain

The inbuilt features make blockchain the most promising technology in the field of distributed IoT applications. These characteristics are depicted in figure 3, and discussed briefly as follows.

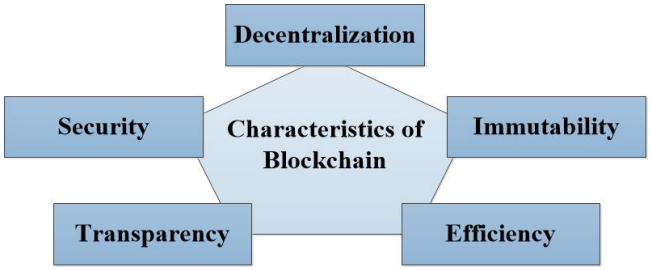

Figure 3. Characteristics of the blockchain.

Decentralization: In blockchain network any node can participate in block creation based on some consensus mechanism. All the connected nodes in the blockchain network can communicate in peer to peer decentralized fashion without any third centralized party. Thus reducing the cost occurred due to maintenance of central servers. As the local copy of the data block is maintained by every node in the network so there is least possibility of single point of failure.

Immutability: All the data transactions performed in blockchain is based on mutual consensus achieved in decentralized autonomous manner. Once the block is added to the blockchain ledger, there is no possibility of modifying the block. Since every new block is linked to the previous block via hashes. If in any case the attacker wants to modify the data block, attacker has to modify majority of nodes in the blockchain. Thus immutable copies of chain of blocks are maintained by the majority every node in the blockchain network.

Transparency: The participating entities communicate in peer to peer fashion based on mutual trust achieved through consensus protocol. Transparency is attained throughout the network, since all the peer nodes maintain an identical copy of blockchain without any third party intermediary.

Security: Security is the prime concern for all the emerging technologies like IoT, blockchain technology when integrated with IoT devices improves the security and privacy of the network. As blockchain

technology uses cryptographic hash codes for every block and maintains the chain of blocks throughout the network life cycle. Nodes are added to the network only after the appropriate consensus mechanism is attained between the participating peers. An attacker has to compromise majority of the nodes in the network while modifying any single data block in the network. Thus enhances the security of existing networks.

Efficiency: Blockchain is resilient network, as nodes perform some computational tasks mutually without any intermediary followed by consensus mechanism. The records are maintained by all the nodes in the network. There is no single point of failure and the system is more tolerant to faults.

The rest of the paper comprises of the detailed survey on the various important technologies and applications associated with the blockchain technology and its integration with IoT networks. Section 2 introduces the extensive survey and comparative analysis performed in blockchain and its integration with IoT upto 2020. Section 3 comprises of the various applications leveraging blockchain with IoT networks. Section 4 reported the detailed research challenges facing in its integration. And finally the conclusion and way forward is discussed in section 5.

2. Literature Survey

In [23] authors defined blockchain a distributed ledger in which data is stored and shared among the peers connected with the network. Blockchain comprises of timestamped blocks which are linked by cryptographic hash functions. The basic functioning of blockchain is based on peer to peer network where all nodes have an interest in using blockchain. Security is the main attribute in blockchain, every node is provided with two cryptographic keys, one public key used by other nodes for encrypting the messages send to a node and second private key used by the nodes to decrypt such messages. Miners in the blockchain network will verify the newly generated blocks are broadcasted into existing blockchain and added to the chain, if not referenced by hash values then these block are discarded. The classification of blockchain based network is done based on some parameters: like type of data, availability, and action to be performed by user. Public blockchain is open to all without any third party and node can act as simple node or a miner node. Miner node will get rewards for functions performed in the blockchain. Some common examples are Ethereum, Litecoin. While in private blockchain all the users are managed by single owner, which restricts network access by deciding about user's control to perform transaction or acting as miners in the system. Examples of private blockchain are Hyperledger-Fabric and Ripple.

In [32] authors described blockchain as a distributed data structure that is maintained among all the nodes that are part of blockchain network. Blockchain was introduced with Bitcoin [33] to perform peer to peer electronic cash system. Blockchain proved helpful with bitcoin to solve the double spending problem [34]. The miner nodes in bitcoin mutually authenticate the valid transactions in the network. The blockchain maintains the states of owners in the network. Blockchain is formed based on cryptographic security of chained blocks in which block is represented by its hashed function and referenced with previous block [24]. Miners are good in resources which take responsibilities in whole blockchain network to decide on the transactions and the sequence in which they have appeared.

Oscar Novo [35] mainly discussed about the main blocks required in any blockchain technology. As the blockchain network consists of the chain of hashed blocks with references to the previous blocks and originating from the genesis block. The genesis block is first initialized block which is always hardwired into the software in the blockchain. There is only one path to the genesis block, although there can be more than one branch (forks) in the blockchain network. The latest block from the longest agreed chain is always chosen. The decision about the longest chain is not based on the number of blocks infact only the cost inquired by the combined difficulty of that chain of blocks. And the shorter chained blocked are considered as orphans and hence discarded. The transaction is basically the transfer of values or simply data between different participating peers which form the blocks. These transactions are mined into valid blocks by special nodes called miners.

Authors in [25] extended the applicability of blockchain technology in IoT networks to further strengthen the trust in process executions without any third party. Blockchain plays a vital role in business process optimization. The smart contract used in blockchain maintains the trust between the parties without any intermediary [36]. Due to the limited resources available with IoT devices make then reliable on third party storage but with cost of privacy. The decentralized blockchain technology will improve the smart IoT based networks in terms of security, storage and privacy [18]. In most of the centralized systems, the main problems related to security and trust based issues were further improved by using the IoT systems in the decentralized and open access mechanism which is possible by using blockchain technology [17], [20]. Blockchain technology is proving to be the most efficient and reliable platform for the decentralized and open access data processing systems [37]. Based on the various survey papers reviewed recently in top journals on blockchain and IoT, Table I specifically highlights core areas and their contribution.

A. Smart Contracts in Blockchain

M. S Ali. et al. [24] described smart contracts as the special type of programmable instructions deployed on blockchain network that govern transactional blocks under set consensus conditions and guidelines, thus acting as a digital equivalent of manual economic contracts between

TABLE I. Overview of Blockchain based Internet of things

Paper Author and Year of Publication	Area covered	Contribution
H. F. Atlam et al. 2018 [28]	IoT, Blockchain	Historical background of IoT and Blockchain. Application areas in IoT and Blockchain Challenges in both.
Xu Wang et al. 2019 [38]	IoT Blockchain	Limitations of IoT security. Blockchain applications. Challenges of applying Blockchain in IoT applications.
Muhammad S. Ali et al. 2018 [24]	IoT, Blockchain	Centralized network architecture for the IoT facing serious challenges. Blockchain and its applications. Issues and Challenges In the IoT. Integration Schemes for Blockchains and IoT.
A Reyna et al. 2018 [39]	Blockchain	Blockchain technology survey, evaluating its distinctive characteristics and open challenges. Identi cation and review of the different ways in which IoT and blockchain are incorporated focusing on challenges, future bene ts. Current frameworks and implementations for BIoT. Evaluation and comparison of the performance of different blockchains in an IoT device.
T. M. F. Caramés et al. 2018 [23]	IoT, Blockchain	Review ways how to apply blockchain to the unique needs of the IoT in order to build BIoT. Further Challenges and Recommendations.
X Wang et al. 2019[40]	IoT, Blockchain	Blockchain based testbed development for IoT to speedup block mining rates.
Imran Makhdoom et al. 2018 [2]	Blockchain	Resolve security and privacy issues of IoT. Identi cation of several special and realistic IoT adoption issues for the blockchain. Study of few emerging technologies and associated voids for blockchain. A path forward to solve any of the important blockchain challenges connected to IoT.
Oscar Novo 2018 [35]	Blockchain	New architecture to arbitrate positions and permissions in IoT, IoT Architecture.
P. K. Sharma et al. 2018 [41]	Cloud and Fog Computing, Blockchain	Proposed distributed blockchain-based cloud architecture, ring low-cost, stable, and on-demand access to IoT network computing infrastructures. Using SDN and BC techniques, a stable distributed fog node architecture takes computing power to the edge gateway level by minimizing end to end delay.
Mark Kim et al. 2018 [42]	Supply Chain Management, IoT	A farm-to-fork, food traceability framework was proposed to combine the Ethereum BC and IoT devices.

participating users. The manual contracts were implemented by the centralized authorities while as the smart contracts based blockchain network does not need intermediaries to establish the conditions. The term 'smart contact' was given by Nick Szabo for maintaining the trust among parties on public networks. Many blockchain platforms have built in smart contracts applications like in Ethereum [43], Hyper-ledger [44]. Whenever blockchain network is deployed then the users can any time invoke the smart contract already present in the blockchain. The smart contacts have their own accounts and addresses in the blockchain [45] thus also termed as autonomous agents. Smart contracts are also associated with some execution fees to avail the functions in the blockchain. Smart contracts are made visible to the participating users in the blockchain network. The smart contracts can be written in various scripting languages depending on the blockchain platform in use, for example Ethereum [43] uses Turing -complete smart contract scripting language written in Serpent and Solidity. These autonomous agents are prone to attacks, as any

loophole in the contact code can prove lethal. In June 2016, Ethereum network came under decentralized autonomous organisations (DAO) attack which resulted in unlawfully tunneling of Ether (cryptocurrency) worth 60 million dollars by the attackers with valid transactions as per the executed smart contract [46].

A. Reyna et al. [39] highlighted that the smart contract code is addressed in the blockchain network by a unique code which users must know first to send transaction. The successful execution of any smart contract is carried with the help of consensus protocol. Smart contracts have numerous advantages like cost reduction, speed, precision, transparency but comes with some vulnerabilities as well hacking, bugs, communication failures. The validity of these contacts is challenging research area which needs gradual improvements [47]. Since more research is to be carried out to identify the conditions in smart contracts which are perceptible for a machine to execute them successfully.

K. Christidis et al. [48] mainly focused on the smart contracts for IoT based applications. Smart contracts are coding scripts stored in blockchain with unique addresses when invoked by address with transaction runs in an autonomous and independently prescribed manner. Smart contracts in blockchain support multi-step processes that occurs mutually between trustless counter-parties. Smart contract's behavior is effectively predictable because of autonomous nature. The IoT devices act as a point of contact with physical world, which are then connected to the blockchain network to automate time consuming work-flows.

In [16] authors mention smart contracts as piece of code which autonomously runs the contractual clause once the set condition is called. It also offers real-time scrutinizing as all the records are stored and verified as transactions in a decentralized topology in blockchain. Smart contract translates IoT devices and other objects into virtual entities in blockchain to be addressed by other entities. IoT nodes security and efficiency can be improved with better coded smart contracts and can perform transactions.

In [49] authors focused on the importance of smart contracts in blockchain network with reference to the various applications. The IoT devices can be coded with the smart contract programming code as per the requirements of the transaction to execute the contract into the blockchain network. IoT device cannot stop the execution of the smart contract once it is deployed in the transactional block in blockchain. In financial transactions transparency and tractability are considered to be the features which can be achieved by smart contract based blockchain technology.

I. Makhdoom et al. [2] extending the blockchain technology to use cases like automatic payments in e-commerce shopping, smart parking, tolls, fuel payment and in digital rights management, and in financial services like capital markets, mortgages, loans, auto-payment of insurance claims. The main idea behind the implementation of smart contracts associated with blockchain technology in IoT devices can maintain operability by paying for the maintenance services. With this the autonomous nature of such a system will pave for development of an ecosystem with efficient and consistent services without any third party.

S Wang et al. [50] efficiently demonstrated a systematic study of blockchain based smart contracts focusing on the emerging application areas in the field of IoT ecosystems. The smart contracts can be simply considered as the protocols that electronically ease the communication setup, authentication, and implement the contracts already shared between the parties under process of communication in blockchain technology. In recent history there were attacks specifically on the smart contracts stored in the blockchain network. Thus main aim of this paper was to present comprehensive research in the area of smart contract which is considered to be the main driving agent in the execution of blockchain technology. The smart contract life cycle is divided into five phases: i) negotiation; ii) development; iii) deployment; iv) maintenance; v) learning and self-destruction. The proposed framework for the smart contracts is considered to be the most practical model for the researchers and finally implementable in the application areas with most secured framework. The research has also highlighted many research challenges which can be further improvised to find the feasible solutions accordingly.

Viriyasitavat et al. [21] stressed upon the importance of autonomous instructions known as smart contracts to reach to some favorable consensus between the peers in the blockchain network to maintain the trust in process execution. Smart contracts results in enhancing the interoperability in IoT networks. The authors have implemented various smart contract modules to achieve consistency among the nodes or validators in the network. More detailed information about the smart contracts like platform languages, security issues and the future intentions are mentioned in Table II.

B. Fog Computing and Blockchain

F. Bonomi et al. [54] proposed the concept of fog computing to provide services like computational power, storage and networking to the end device in the IoT ecosystem before moving to the cloud based systems. Thus bringing all these services close to the edge devices which improves the latency, high availability in real time applications. A. Seitz et al. [55] extended the fog computing services to the blockchain based internet of things in mostly industrial domain. Blockchain technology helps in providing the transparency between all the participating entities in the network and also the traceability of the objects on edge devices. Mostly the IoT devices have resource constraints; hence require some special nodes which will take responsibility of integrating these end devices with the blockchain network. These special nodes are designated as fog nodes. A complete prototype was demonstrated with most technologies

TABLE II. Smart Contracts in Blockchain based Networks

Paper	Contribution	Smart Contract Language	Platform	Security Issues	Future Intention
M S Ali et al. 2018 [24]	Overview of smart contracts only	Ethereum	Solidity	Design issue:contract deployed with bugs and loopholes, DAO attack in 2016 with losses around 60 million dollars.	Not addressed
A Reyna et al. 2018 [39]	Overview,advantages,scope for new applications	Ethereum	EVM code, stack based bytecode	Design issue:contract deployed with bugs lead to hacking,viruses and communication failures.	Correctness and control logic validation, smart modeling of conditions into contracts
X Wang et al. 2018 [16]	Translation of IoT devices and digital assets into virtual identities, e cient and secure method	Ethereum		Vulnerabilities: transparent bugs and frauds with irreversible deployment of contracts	Not addressed
S Moin et al. 2019 [18]	Case study of Insurance smart contract	Ethereum		Hacking, malware, bugs and ambiguous receipt of details	Security breaches must be addressed
Y Zhang et al. 2019 [13]	Smart property use case, minimizes fraud and intermediary cost	Not addressed		Not addressed	Uniform data format with credit and ranking system
I Homoliak et al. 2019 [51]	Overview, Only Bytecode is public not source code	Ethereum	Serpent, Solidity	Vulnerability exists due to invalid code sometimes	Amending security issues
S Malik et al. 2019 [52]	Smart contract for automation of reputations in SCM in a secure and e cient manner	Hyperledger		Bad mounting attack and impersonation	Throughput and latency improvements
K Chrishdis et al. 2016 [48]	Detailed working of smart contract	Ethereum	Solidity	Not addressed	Integration of new business models with blockchain and IoT
S Wang et al. 2010 [50]	Detailed working of smart contract, use cases	Ethereum	Solidity	Immutable bugs, less trusted data feeds, privacy issues	Formal veri cation, Societal and organisational impact on smart contracts
H Desai et al. 2019 [53]	Smart contracts for Publicly available Auctions and Bids. Detailed algorithms for creating and deploying smart contracts	Ethereum,Nodejs,npm, Tru e,Web3js, Remix for deployment	Solidity,	Privacy Violations: disclosing all bid to auctioneers	Framework for varied applications with multiple blockchain, preserving privacy

included at each level of architecture. Fog devices were able to process the data from IoT objects using Intel Next Unit Computing (NUC) tiny device capable of performing majority of the tasks then interfaced with private Ethereum blockchain. The main motive of using blockchain in the prototype is to maintain transparency and visibility for all the stakeholders in the network. The further improvements of the proposed system are enabling smart contracts for the autonomous micro-payment systems. The main drawback raised while implementing blockchain technology is due to the lack of expert knowledge and the execution and validation time of blocks in the system was too high.

R. Brundo et al. [56] mainly focused on the potential adoption of blockchain technology in the existing cloud and fog based systems to make them more transparent and decentralized systems without any involvement of less trusted intermediary systems. The authors carried out extensive study of three main projects based on the said domain and nally evaluated varied observations as mentioned: Golem based crowd funding project's motive is based on decentralized supercomputer using blockchain technology, iExec blockchain based decentralized cloud and SONM

(Supercomputer Organized by Network Mining) focused at a decentralized fog supercomputer. There is dearth of acceptance of these technologies thus intensive research must be carried out in the eld of blockchain based cloud or fog projects. The research areas include: lack of standards, validation of the results of computation, specifying the benchmarks for provider's resources.

M. Li et al. [57] proposed a blockchain based vehicular fog computing for sharing cars by passengers while travelling to reduce time, less carbon emissions and no frequent tra c congestion. The passengers will prefer local drivers and relying on the remote cloud servers will add more latency and communication overhead. Thus a fog computing somehow reduces the overhead and latency but the security and privacy of these passengers is of great concern. To address this problem of privacy and mistrust, the authors have proposed an e cient carpooling scheme based on decentralized blockchain technology. The proper validation and proofs of consensus between the passengers to carry out the task by maintaining the anonymity in the communication. Private blockchain stores the carpooling records in a veri able ledger to provide data auditability. The system is lacking further data veri cation mechanisms whenever disputes like claims and proofs from users arise and needs proper veri cation by the witnesses. Public blockchain or consortium blockchain involvement is in consideration for carpooling to add more dimensions the proposed system.

P. K. Sharma et al. [41] proposed a software de ned fog node based blockchain cloud architecture for internet of things aimed at dealing with huge amount of data generated by these IoT devices managed by the distributed cloud based servers. The proposed model proves to be bene cial for IoT ecosystems. It brings the processing close to the edge devices thus achieves low latency and easy availability of the resources to the nodes requesting at any instance of time. The cloud based services are maintained in distributed and decentralized manner in blockchain network. The outcomes when compared with the existing models signi cant improvements based the parameters such as latency, reducing response time, increasing throughput, and capability to detect the attacks in real time with compromised performance overheads.

C. Consensus Mechanisms

Consensus algorithms [23] acts as the main driving force to execute the blockchain technology in a decentralized manner between parties in communication by maintaining anonymity. It is basically the set of agreed upon instructions that determine the conditions to be attained, so that the agreement is ful lled for validation of new blocks into the blockchain to carry out the transactions successfully. The consensus algorithms in decentralized networks provide visible solutions to the Byzantine Generals Problem [58]. The right decision about the inclusive attacks to be ordered by the generals about the emergency noti cations about the attack provided by multiple parties was very di cult. Di erent algorithms were proposed to create the consensus among the di erent parties in a tamper proof manner without relying on the third party.

The authors in [39] discussed that the consensus protocols maintain the data integrity within the blockchain network. In Proof of Work (PoW) based consensus protocol, the miners will have to perform challenging tasks rst then only the block will be accepted for transaction. The participating peers will add new block, and the longest chain of blocks is considered as the valid on the basis of cost inquired in its computation. Energy consumption is the main limitation in the PoW protocol. The limitations like high latency, high energy costs and less transaction speeds of PoW restricts its applicability to many application areas. Another alternative consensus mechanism in blockchain technology is the Proof of Stake (PoS). PoS states that the peers with more coins will be more interested in performing transactions by securing the interactions in the network. Many consensus mechanisms have been proposed but mostly without much acceptance in the blockchain network. Thus main focus is to be carried out in the eld of research in validating these consensus mechanisms to practically legitimate in blockchain technology.

The authors in [24] reviewed various existing consensus algorithms in detail. Consensus algorithms acts as main challenger in accepting the block and maintaining the coherence and synchronized states as per the agreed procedures among the peers in the distributed manner. The authors discussed consensus algorithms applicable in the permissioned and permissionless blockchains. The main motive of the study was to nd out the applicability of public or private blockchain consensus mechanisms when applied in IoT use cases. The main problem of voting based consensus permissionless blockchains can provide easy access to anonymous peers which can lead to Sybil attack. Thus lottery based consensus mechanisms where followed to select the node that can publish the block in the blockchain. The participants are unable to forcefully make consensus decisions in its favor because of cost associated with each block creation. The transaction fees claimed by miners for creation and validation of new blocks in the blockchain network adds more security against false block creation and distributed denial of services (DDoS) attacks. PoW cannot guarantee the synchronization of execution of blocks from di erent locations which resulted in the creation of orphaned blocks. The chance of 51% attack arises as node can seldom take charge of 51% of processing power. It takes more time to nalize the block in the network and can be rolled back to previous state in 51% attack. Once nalized it is impossible to roll back. Ethereum transactional block is nalized after six con rmations which takes nearly two minutes. The Proof of Stack (PoS) based consensus mechanism is quicker and less energy consuming than PoW protocol. The validator node selected pseudorandomly takes the responsibility of block creation in the network. In PoS consensus mechanism block nality is

TABLE III. Trending Consensus mechanisms used in blockchain based IoT systems

Paper	Contribution	Parameters	Comparison/Limitations	Outlook
A Panareela et al. 2018 [11]	Overview of Consensus algorithms:PoW, PoS, Casper, DPoS, PoC, PoET, Algorand, SCP	Computation and Validation rule PoW: Difficult to solve but simple to verify, PoS: Stake based leader selection, Casper: Bonded validator, DPoS: Deterministic leader selection with Round Robin, PoC: Harddrive storage for solving cryptographic challenges	No comparison details	Scalability issue with IoT integration
Z Zheng et al. 2017 [59]	Focus on Byzantine problem, PoW, PoS, PBFT, DPoS, Ripple, Tendermint	Selection and fault tolerance PoW: Miners perform complex calculations, PoS: selection based on currency, PBFT: Tolerant upto 1/3 of faulty nodes, DPoS: Democratic selected delegates to validate blocks	PoW: Wastage of time and power, PoS: Prone to attacks due to zero mining cost, PBFT: Compromised if >1/3 faulty nodes, Ripple: problematic when >20% faulty nodes	Scalability
M Xu et al. 2019 [60]	Detailed discussion on Consensus algorithms:PoW, PoS, DPoS, Proof of Luck, PoC, SpaceMint, PoA, PoB,PBFT Tendermint, Ripple, SCP	Type, Transaction Finality,	detailed comparison of protocols	New consensus models
M S Ali et al. 2018 [24]	Detailed discussion on Consensus algorithms:PoW, PoS, Hyperledger Sawtooth, PBFT, Tendermint, FBFT	Safety, Liveness and Fault tolerance	Block Finality: PoW requires 6 confirmations which takes 60 minutes in Bitcoin, 2 minutes in Ethereum, and 1 second in Tendermint	Scalability
W Wang et al. 2019 [37]	Mathematical modelling on Nakamoto Consensus Protocols	Correctness, Consistency, Liveness and Total order	detailed comparison of protocols	Decentralization cost, multiple party computation jointly on blockchain
T M Fernández-Caramés et al. 2018 [23]	Comparison of various consensus algorithms from literature:PoS, DPoS, TaPoS, PoA, PBFT, DBFT, Ripple, Stellar, BFTRaft, Sieve, Tendermint, Bitcoin-NG, PoB, PoP	Throughput, Energy consumption, Scalability	No comparisons mentioned	Decentralization cost, multiple party computation jointly on blockchain
X Wang et al. 2019 [16]	Overview of consensus mechanisms: PoW, PoS, PoA, PoB, PoI, PBFT	Principle to validate unit data, structure of unit data in BC ledger	No comparison between consensus algorithms discussed	IoT specific Consensus algorithms

TABLE IV. Comparative Analysis of Consensus Mechanisms

Consensus Algorithm	BC Type	Block Finality	Vulnerabilities	Computational Cost	Scalability	Latency
PoW	Public BC	Probabilistic	51% majority attack	High	Low	High
PoS	Both	Probabilistic	51% majority attack, Monopoly of credit rich nodes	Low	Low	Low
DBFT	Private BC	Instantaneous	33% Faulty nodes	High	Low	Low
PBFT	Consortium	Instantaneous	$n/3$ Faulty nodes	High	Low	Low
DPoS	Consortium	Probabilistic	50% majority attack	Low	Low	Low
Ripple	Consortium	Deterministic	more than 20% faulty nodes in unique node list	Low	Low	Low
PoET	Public BC	Probabilistic	51% majority attack	High	Low	High
Tendermint	Both	Instantaneous	more than $n/3$ Faulty nodes	Low	High	Low
Algorand	Public	Instantaneous	dishonest nodes having more than 66% of total money	Low	High	Low
Sieve	Private	Deterministic	dishonest nodes having more than 66% of total money	Low	High	Low
Stellar	Public	Deterministic	behaves inactive during malicious behaviour	Low	Low	Low

much quicker than the PoW but can be posed with serious attacks, thus needs further improvements. The permissioned blockchains allow only limited users to retain the copy of complete blockchain. Since there are less chances of Sybil attack because of known participants, thus voting based consensus mechanism is followed. Practical Byzantine Fault Tolerance (PBFT) is an optimized and encrypted data exchange based voting mechanism in practice. In PBFT consensus algorithm, one node is selected as the leader which which collects all the transactions in the block and forwards to all nodes in the network. The peers validate the blocks by calculating their hash values and transmits them back to the network. The validating peers examine the hash received from the rest of peers in the network and treated as votes over number of rounds, if two-thirds are supporting the candidate block then peer nodes will accommodate it to their local copy of the blockchain. It attains low latency and high throughput but comes with the limitation of handling more number of nodes in the network. Tendermint is a BFT consensus algorithm very much similar to the PBFT provides $p \quad 3 f + 1$ fault tolerance where p is total processes and f is the number of faults. It uses PoS with the PBFT consensus algorithm to provide high throughput, more security, and low block processing time. Tendermint further provides guarantee against con icting blocks and no forks creation in the blockchain network. Transaction nality about one second in Tendermint and can be used both in private and public blockchain. The comprehensive survey is carried out on the latest research in the area of consensus mechanisms in BIoT in a precise manner which is depicted in table III. The comparison is based on the most distinctive parameters discussed with future intentions for the researchers. The table IV also differentiates among the famous consensus protocols followed in most of the blockchain platforms.

D. IoT and Blockchain Architectures

1) IoT Architecture

As there is no common consensus about the globally accepted architecture for internet of things. However 3-tier architecture for IoT is commonly followed by the researchers [61]. It consists of the Perception Layer managing the physical devices by capturing the data from

Figure 4. Architectures for IoT[62], [63].

the environment, the Network Layer provides the internet communication and routing mechanisms and the Application layer provides the ways to connect to the different application domains. Application layer acts as a front end for whole IoT ecosystem to provide information seamlessly. The three-tier architecture for IoT networks presents the basic idea for its implementation but no detail about the management and adaptation layer capabilities.

IoT ecosystem [2] has shown tremendous improvements in the terms of application uses cases, software and hardware technology, enabling technologies and IoT specific communication protocols, still there is no common consensus between different researchers and the organisations in terms of a universal architecture for IoT. Various IoT architectures have been proposed by researchers from time to time relying to the expectations of particular constraints and the application use case. The heterogeneity of the IoT devices from the multiple vendors and diversified use cases makes it more difficult to come with the single IoT reference model [62]. A five layer IoT architecture in Figure 4 consists of objects or perception layer which acts as the device layer comprises of physical components like sensors and RFID devices. It is responsible for capturing data from sensors then forwards it to the object abstraction layer.

Qiu et al. [63] presented four layered architecture for IoT networks consists of sensing layer, networking layer, cloud layer and application layer. It has also provided some solutions to the self-adapting, big data analysis, privacy. The cloud layer provides more availability of resources, thus handles huge data analysis. Interoperability is the major challenge for middleware layer because of using proprietary protocols.

2) BIoT Architecture

In paper [35] the author focus on the design of general architectural framework for IoT using blockchain technology by removing the centralized access management which was single point of failure in most of the cases. It applies a specialized design approach by using single smart contract at access control layer explaining the entire process by reducing communication overhead in blockchain network. The important parameters like scalability and better results considering lightweight IoT devices. The blockchain's decentralized, secure and autonomous characteristics make it a perfect component to become an integral component of the IoT solution. The decentralized architecture uses blockchain technology as the access control mechanism for data exchanges and storage. The IoT devices are mostly constrained in nature and are incapable to store the complete blockchain. In this architecture, the management hub takes care of requests from the IoT devices into the blockchain network. The architecture depicted in Figure 5 comprises of various elements explained precisely.

A. Dorri et al. [12] proposed a light weight based architecture for IoT use cases using blockchain technology considering the resource constraint nature of IoT devices while blockchain utilizes high bandwidth and communications delays. It is based on hierarchical overlay network using cloud services. Smart home use case has been studied and the main motive of integrating blockchain technology is to provide privacy and security. The proposed model comprises of smart home which includes various IoT devices like thermostat, smart bulbs, IP camera etc. The local blockchain will be maintained in smart home by high resource devices which will act as miners. These miner nodes are connected to the overlay network by Tor [64] to maintain further anonymity in the network. Cloud storage will store the hash of stored information with proper block number identifiers for further decision making analysis. In the architecture, there is more overhead due to cluster head selection criteria in overlay network.

3. Blockchain Based Internet of Things Applications

The main properties like decentralization, transparency, security and immutability in blockchain technology has shown keen interests in its integration with IoT based applications. Blockchain technology is not confined to the cryptocurrency but shows rapid improvement and acceptance, when applied to various real world scenarios especially in IoT ecosystems. Let us briefly discuss here some of the Blockchain based Internet of Things (BIoT) applications that have been proposed in the literature.

A. Supply Chain Management (SCM)

SCM is the backbone of majority of modern business establishments. The life cycle of any supply chain should provide all transaction updated about the products, authenticity and transparency throughout its delivery by the actual consenters. Blockchain technology is considered to the promising alternative to maintain transparency, immutability and security in SCM with decentralized framework [65], [20]. Tracking of food items is the main application in SCM which includes IoT devices and be further integrated with block chain technology. Chinese government decides to integrate blockchain with the supply chain of beef imported from various locations of world. In order to guarantee the safety, transparency, traceability and immutability of these food items [15]. The food items were equipped with IoT based devices (RFID, Sensors, actuators etc.) for continuous

Figure 5. Blockchain based Architecture for IoT[35].

collection of data in the supply chain. The data is stored in the blockchain, which maintains the distributed ledger of all the transactions carried throughout the lifecycle of the supply chain to achieve traceability, safety and sharing of actual information in entire supply chain. In another approach [32] authors formulated a blockchain model for improving supply chain systems. A multiple agent system was introduced which included all the participating entities like producers, processing units, transporters, retailers and consumers in the supply chain. The smart contract is the main deciding factor between different agents in a circular economy with recycling features. Block chain technology has been integrated with supply of diamonds to prevent any fraud starting from the sender which are digitally signed and stored in distributed ledger using blockchain technology [2].

S. Ramamurthy [66] highlighted the research work carried out jointly by IBM, Wal-Mart and Tsinghua University to propose an efficient supply chain management. All the transactions are stored in a distributed ledger using blockchain technology while maintaining the authenticity, transparency, and traceability of the actual information stored about the foot items maintained throughout the supply chain. The consumers, retailers, and government agencies can monitor the supply chain as per the consensus mechanisms maintained between the participating peers in the network. Authors in [67] relies on the transparency and updated links created in supply chain using blockchain. The blockchain and IoT integration in SCM maintains traceability and informative systems with easy accessibility.

Authors in [68] worked on Pharma based supply chain to monitor the delicate parameters associated with medicines while in transit for maintaining the quality control in the system. The world epidemics specifically Covid-19, which is presently unstoppable and no vaccine has been developed for this dreadful disease. But the various government and health organisations throughout world are working day and night to control the further spread, which can be possible by the real-time supply chain management of necessary protection of items and testing and controlling equipments. These global epidemics have direct impact on the overall supply chain throughout world. As per survey, China is the largest manufacturer and exporter of majority of the goods worldwide. This has created supply chain crisis in many companies [69]. The modern day SCM must possess the features like decentralization, transparency, traceability, security and immutability which will maintain the global ledger and adjusting the multiple parties to fit in the supply

Figure 6. BIoT Applications[35]

chain.

B. Autonomous Firmware Updates

Most of the IoT based devices require regular software updates in order to improve its functionalism by continuously removing bugs with newer rmware updates. The blockchain technology helps in mitigating the valid rmware updates after the approval of transaction updates after due process of validation and mining in the approval of transaction update in the blockchain network [2]. Authors in [70] focused on the embedded devices used in most of the IoT ecosystems. Most of the operations are carried out autonomously in machine to machine communication which requires regular secure rmware updates with improved functionalities and better performance using blockchain technology. Whenever any IoT device requires an update, it will request all the nodes in the blockchain network which after due validation and veri cation provides the rmware updates to the requested node. Bittorrent is used as peer to peer rmware downloading platform. There are various security issues like Man in the Middle attack and rollback attack which can come across while uploading any rmware instruction on the IoT devices. The authors in [71] proposed new rmware management architecture based on blockchain and inter planetary le system to resolve security issues and securely install the updated rmware version on the devices.

C. Smart Health

Blockchain technology has shown signi cant development in its integration with the medical health related applications mostly using IoT devices for data collection and sharing. Various organizations are working on its integration with IoT systems in smart health [72]. Blockchain technology is able to provide seamless availability of information sharing between patients, doctors, medicine suppliers and various associated departments in maintaining security and privacy [15]. Authors in [73] carried out extensive survey in identifying the importance of blockchain in health care related use cases. The medical records related to diseases, patients, reports, human body examination scans, when made available to the world renowned researchers and organizations can be taken of good human use. Blockchain processes the property of improved security, trust, immutability, ownership, availability, and transparency. Authors in [20] considers healthcare as the main pillar for the overall development of any nation in the world. With the huge amount of medical records about the medicines, symptoms, diseases, conditions and reports etc. becomes a challenging task to disseminate and store securely. Block chain technology integrated 5G enabled IoT systems which de nitely change the scenario of dealing and sharing healthcare related use cases. It maintains a distributed, immutable, transparent and secure management of information in the network.

In [74] authors also reviewed the use of blockchain healthcare management system to maintain a distributed and transparent Electronic Health Record (EHR) throughout different medical institutions, medical supply chains, and pharmacists in a secure manner. The various blockchain based smart healthcare systems like MedRec, Gem, SimplyVital Health, Hashed Health System, Healthcare Working Group,

and Robomed Network were also mentioned. Authors in [75] proposed MeDShare which a trust-less smart health care system in which patient's medical information can be shared in a secured and transparent manner only using blockchain technology. MeDShare is based on autonomous smart contracts and follows a well de ned access control system which e ciently monitors the pattern of the nodes and can easily revoke the access in a tamper proof manner. Authors in [76] mainly focused on the interchangeability issues in most of medical databases in UK. The main reason for the non-availability of these huge medical records is due security and privacy of concerned data owners. The authors focused on the integration of these EHR with the blockchain technology, which will be resilient in maintaining the security and privacy in a distributed, transparent and immutable manner.

D. Smart Industries

Industrial internet of things (IIoT) is speci cally meant for automation and management of all industrial processes that includes supply, manufacturing, processing, maintenance, and business decision capabilities. IoT has transformed the way of dealing with existing industries for generating more revenue and environment friendly solutions. These IIoT systems mostly rely on centralized services which is the major bottleneck, as it can be single point of failure and maintaining privacy and security is hard to achieve while carrying transactions on intermediary systems. Thus blockchain technology can be integrated with IIoT based systems achieve privacy, transparency, security and traceability as per the consensus arrived by the participating peers in the decentralized network. Authors in [20] focused on using BC with business processes in various industries to maintain trust by the participating parties and reduce the overall cost by removing the intermediaries with improved transaction nality and transparency. Authors in [77] integrated the BC technology with IIoT in maintaining a distributed autonomous framework in a secured and transparent manner. As the IoT devices are resource constrained devices some complex processes like mining of complex consensus mechanisms (PoW) must be added to cloud based services which is dicult to be processed at the device level.

E. Smart Cities

IoT signi cantly improvised the management of complex tasks in majority of the modern cities in world. As huge tra c and human population is seen in these urban areas which is very challenging to manage and coordinate the real-time control and analysis in various essential services like transport, health, waste and sewage, Energy, Water, Environment, Safety and Security, Disaster management, eGovernance. Thus smart city collectively manages are the services within its scope in order to provide adable and e cient services. IoT is incapable in maintaining the security, privacy and transparency in distributed manner without any new innovative enabling technologies like blockchain. Blockchain technology maintains a distributed database on a decentralized platform in achieving transparency, privacy, and security of the delicate details available in the network. Blockchain technology has a signi cant impact on its integration IoT based networks in managing smart cities [9]. Authors in [20] have highlighted various challenges faced by the IoT based smart cities use cases. The blockchain based smart cities were discussed to maintain the security and privacy in a trust-less and distributed manner. The vehicular tra c in smart cities can also be managed by using blockchain based distributed vehicles in ce ciently and transparent way without trusting on a single centralized service [2]. Furthermore the blockchain technology has strengthened the security and sustainability of smart cities in sharing economy based on autonomous smart contracts in cyber physical systems [78].

F. Insurance Services

Majority of the insurance companies are unable to detect the frauds and misleading claims which costs them millions of dollars. Blockchain technology autonomously controlled by smart contracts can be bene cial in automating the insurance claims as per the consensus achieved by the participating parties in a distributed and transparent manner [50].

G. Smart Homes

IoT based smart homes maintain seamless interconnections are the essential services and appliances to optimize and control via smart devices or web-portals over internet. The security and privacy is still the major concern in IoT based networks. Security and privacy can be maintained by using blockchain technology [11]. Authors in [8] proposed a blockchain based model for smart homes, in order to improve the autonomous interaction with reduced costs and energy savings. Blockchain technology maintains security and privacy IoT based smart home use cases which can easily managed in distributed manner [12]. Authors in [20] discussed various blockchain based smart home models. The immutable feature of blockchain network makes the attackers unable to modify the data in the chain of blocks stored in distributed ledger. The latency related issues can be improved by using 5G based wireless communication technology. The authors have somehow further improved the security and privacy issues by creating various policies related to smart contracts applicable in smart home systems. Authors in [79] mainly focused on the lack of trust between multiple parties in a centralized system are more vulnerable to security and privacy breaches. Thus a continuous security system is maintained IoT by using blockchain technology. Crypto based tokens were used for authentication purposes which increases the security without any third party service.

H. Digital Records and Rights Management

Blockchain technology incorporates transparency, security, immutability backed by a decentralized network to maintain a distributed ledger which can store records of entities like goods, credentials, digital rights [9]. Authors in [20] highlighted the importance of protecting digital

rights of multimedia like text and images. Digital rights management systems were reviewed. In one blockchain based model, the active right owners can directly interact with the system after the authentication using blockchain technology. And the second model using smart contracts for the various copyrights management in real-time using cryptographic hashing techniques to con rm all transactions in a transparent and distributed manner. Authors in [50] discussed the importance of implementing blockchain technology in preserving all the contract properties and rights as cryptographic certi cates which can be managed by smart contracts running in these networks. Real estate properties integrated with blockchain such as Propy -su ciently improves the security and transparency between the participating entities without any untrusted third party.

I. Rental Accommodation and Utilities

Authors in [48] highlighted the usage of blockchain in renting various services and properties to the needful users in generating the revenue. Authors in [11] mentioned the Slock.it [80] platform which is blockchain based IoT service. The smart devices can be made available as a service on rent after due process of consensus managed by smart contracts. The users using these rented devices will have to make some payments as per the usage of the service.

4. Challenges in Implementing Blockchain in IoT

In this section we will rst describe the research challenges in the large scale adoption of IoT. Moreover, integrating the architecture of blockchain in the IoT has its own challenges. Those challenges are also listed in this section.

A. IoT : Challenges

IoT based systems are becoming complex with the advent of new enabling technologies and direct involvement of IoT in daily lives of human beings. The various factors which have an impact on the humans include security, safety, privacy, health, mobility, energy e ciency, environmental sustainability [3]. Thus main challenges from various aspects like enabling technologies, applications, and architectures in IoT networks must be taken into consideration for a viable solution which can be successfully implemented. Some of the signi cant IoT challenges are:

Standardization and Architectures: [3] IoT systems are based on multivarious technologies and standards. Standardization of IoT architecture and communication standards act as a driving force for its development. Open standards are easily available in the public domain for collaborative enhancements based on the consensus for better interoperability using varied standards. Thus open standards can be play successful in the deployment of IoT ecosystem. Furthermore there is no consensus between di erent organizations and the researchers about the universally accepted architecture for IoT networks. Mostly follow three or ve tier based architecture for IoT network.

Scalability: Scalability is considered to be the important challenge in IoT which must ful lls the adaptability of more and more IoT devices connecting to the existing IoT network. It implies the network capability to deal with immense growth of network infrastructure by adding more devices and services to the system without degrading overall performance of system. Thus scalable mechanisms must be adhered to adjust more devices with seamless connectivity and adaptable topology [3]. Scalability issue is still a research area to validate the potentials of the IoT ecosystem when enormous new devices are joining the existing network.

Security and Privacy: The security and privacy is the main challenge in establishing the IoT networks in vast domains. The IoT devices in the IoT ecosystem are made accessible anywhere in applications across organizations and di erent service platforms. Some IoT systems are connected to critical lifesaving applications which are connected through the internet. Internet is main attraction for the attackers which may bring catastrophic problems in these industrial or human well-being IoT systems with life implications [81]. The pervasive nature of IoT networks makes them more susceptible for attacks like sni ng, replay attack and DoS attacks. These attacks are somehow impossible to trace while examining the digital evidence [82].

Interoperability: Interoperability logically acts as a common interface for millions of IoT devices from multiple vendors regardless of the hardware and software. There is heterogeneity in the standards and the technologies from di erent makers of these devices and thus it is di cult to streamline the operations throughout the all the layers of IoT architecture. It becomes a fundamental priority to maintain interoperability within the IoT system at a cost of some cutting edge technologies.

Heterogeneity: With the advent of IoT technology, heterogeneity came into limelight because IoT ecosystem comprises of billions of IoT devices from di erent manufacturers with varied hardware and software. Thus main aim of the researchers and the IoT based organisations is to build a common consensus in smooth functioning of the operations in IoT networks [28]. The platform services in the IoT system must accommodate with each other while dealing with varied hardware and software of IoT objects and the network and communication protocols.

Real Time Operations: In most of the IoT use cases, timing is a deciding factor while executing the various processes in the network and sort of delay can prove fatal like in e-health applications where pacemakers are monitored by IoT devices and in industrial ap-

plications many sensors and actuators are monitoring and controlling the costly machines [81]. There must such programming functions in the operating systems which must take these time critical processes on priority which any delay.

Transparency: Information sharing is the main goal of IoT networks, but no clear cut information about transparency while performing the operations and what will happen to the personal information shared by the users about who can access and with whom it will be shared to advertisers and third parties. It is important to maintain transparency by mentioning the rules and guidelines for the valid use of the information and the security data or metadata.

Centralized System: The centralized systems face a major problem of single point of failure, which can result in many issues such as data recovery, theft of data etc.

B. Blockchain in IoT : Challenges

Blockchain technology is still in the infancy and facing multiple challenges in its development and integrating with IoT networks [24]. Blockchain network was meant for internet based networks which can be connected in distributed manner mostly with good computational power. Initially blockchain technology was focused for peer to peer homogeneous networks, in which the nodes have capability to validate and store the block [16]. As IoT devices are mostly resource constrained in nature which becomes challenging for integrating with blockchain technology [39]. Mostly blockchain technology is facing following important challenges while integrating with IoT applications:

Scalability: The participating users in the blockchain network after positive consensus have to retain the whole copy of the transactions as chain of blocks in their memory [24]. It de nitely have advantages by providing decentralized access, fault tolerance, security and immutability but scalability comes out to the main challenge in blockchain technology. As the number of participating users increases, the size of block also increases which burdens as the computational cost. The consensus based algorithms will manage the transactions to be carried out in blockchain at optimal level will restrict additional nodes to be incorporated in the network as it requires more computational power to perform the transactions on time. As IoT devices are mostly limited in computational cost, storage, and networking capabilities which will add more problems to the blockchain based IoT network. Researchers have proposed various ideas in order to improvise the scalability issue in IoT network with blockchain technology. Many architectural models are being studied in order to increase the scalability like multi-tier blockchain architecture [83] which implies resource limited nodes are connected to public blockchain network via IoT gateways. Some solutions suggest ooading the processing, storage to some o chain based network [84] and consensus mechanism to dierent parts of blockchain network in an inter-connected network of blockchains [85]. Scalability still exists as main research challenge in leveraging blockchain technology with IoT based network applications.

Computational capabilities: Computation becomes main challenge while adopting blockchain technology into IoT ecosystem. Majority of the IoT devices have scarce resource which are incapable in dealing with the blockchain processing and storage. The consensus algorithms like PoW is won't work properly in IoT devices. Normal GPUs can process 107 hashes per second while and Raspberry Pi 3 (IoT device) can compute 104 hashes per second [16].

Storage Management: Storage is also among the main challenges in blockchain technology on applying IoT uses cases. As the size of valid chain of blocks grows gradually over the period of time in blockchain network. Since IoT device are resource limited devices which becomes very problematic to implement blockchain among the users in IoT. The IoT devices require the details of historical data to process the further transactions in the blockchain. Blockchain technology has improved in meeting the demands of these constrained IoT devices by making some provisions in which the IoT devices can act as light nodes. The light nodes do not save the whole block but will save the block headers only [16].

High Latency and Low Throughput: The processing time of transactions in blockchain network is very high as compared to the existing online nancial transactions. VISA based networks can handle around 24,000 transaction per second while as Bitcoin blockchain can handle 7 transactions per second. The consensus to be achieved about any transactional block will take time in order to maintain consistency, avoid double spending problems will result in low throughput [23]. Blockchain technology is famous for its transparency and consistency to be maintained in decentralized manner, which results in high latency. It is acceptable in many blockchain based networks but somehow infeasible in time critical IoT applications e.g. VANETs [16].

Trade-o in Public-Private Blockchains: Blockchain technology is still behind the mainstream nancial systems like Paypal in terms of performance. There is also variation in performance within private and public blockchains. Private blockchains are faster having high transaction rate which results in high throughput as compared to public blockchains. The public blockchains provide complete decentraliza-

tion framework which is not possible in private blockchains because these are governed by the organization itself. Private blockchains uses voting based consensus mechanisms while as public blockchains rely on lottery based consensus which adds latency in selecting valid blocks from the open parties in the public blockchains. Blockchain maintains tradeo between transaction throughput and the decentralization structure. As IoT ecosystem is connecting multiple geographical regions which needs mutual integration of various blockchains in order to provide the quality services with improved performance [24].

Anonymity and Privacy in Public Blockchain: Most of the IoT applications deal with con dential data like in smart health, smart-homes, smart-cities etc., it becomes prime challenge to maintain anonymity and privacy of the individuals taking part in these environments. Blockchain hopefully addresses the identity management in IoT networks by hiding identity while sending the personal data over the network. Since IoT devices are limited with resources, it becomes more challenging to incorporate security mechanisms at the device level [39]. The public blockchains are more transparent which record transactions and all participants are able to visualize these transactions. The attacker can extract inferences from these records which can reveal user information. Zerocoin blockchain speci cally enhances the privacy by enabling the anonymity between peer to peer transactions [24].

Legal Issues: The legal regulation of most technologies is still a dream. Data privacy play vital role in maintaining the data integrity. There are some regulating statutory bodies but in practical, organizations work di erently. There is need of new laws and standards can help in maintaining data privacy and integrity. It is still a big challenge in dealing with IoT systems with blockchain technology incorporated in it. The new laws can also restrict the openness of decentralized blockchain networks [39].

Choosing Appropriate Consensus Algorithm for IoT: The resource constrained nature of IoT device makes some consensus algorithms more dult to implement in blockchain based IoT networks. PoW is unsuitable for IoT devices to perform the activities of a miner or complete node. In order to incorporate the consensus algorithms several solutions suggest that the high end processing will be done on gateways or by the resource full devices [39].

Maintaining Security while Programming Smart Contracts: Blockchain technology is eminent for the inbuilt security mechanisms which include cryptographic algorithms. The smart contracts act as triggers means an autonomous programming instructions performing critical transactions in the blockchain based IoT networks. Any loophole in these smart contracts will have severe implications on the whole network. An adversary can use these weaknesses in the smart contracts to unlawfully extract information or perform nancial transaction. Thus research is to be carried out in nding some security enhancements in the smart contracts which will protect it from any adversaries attacking the BIoT network [24].

Big Data and Machine Learning Approaches in BIoT: The advent of machine learning has improvised almost every eld of science and technology. It has totally changed the shape of IoT ecosystems as well by various developments in eld of autonomous smart cars, smart health care, and smart-cities. Machine learning can be productive while applying on various IoT applications. In IoT, Machine learning will change the way-out of how to make best decisions. It will provide intelligent decisions by optimizing the automatic processes in various IoT applications to manage and perform the operations with precision and accuracy. Machine learning has huge potential in the applications like online transactions, asset management, scheduling and intrusion detection systems in IoT systems. Arti cial intelligence at edge devices in IoT use cases will maintain trust while collecting data from the users which may include the attackers and remove the redundant data at the gateways before transmitting it to further higher layers. Machine learning extension can be further seen as an asset in blockchain based IoT ecosystems [24] in order to apply various machine learning models to the huge data received from millions of IoT devices. The decentralized, transparent and distributed nature of blockchain will help in making the voluminous data available for open collaborative IoT systems [38]. The big data repositories available for the users secured by blockchain technology can help in eient training for autonomous systems. Blockchain technology can be helpful also for critical big data repositories like medical records to enforce access control mechanisms which are important in IoT applications. Thus the further combination of big data and machine learning to the BIoT ecosystems will be very productive in future.

5. Conclusion

The security, privacy and the third party services are still the serious challenges in IoT systems. Since IoT is the backbone of the modernized seamless and autonomous information and communication technologies, the challenges faced in these systems force the researchers to experiment for new innovative technologies which will further improvise the interactions with these systems. Blockchain technology is considered to be among such trending platform which can o er such services while integrating with IoT networks. We discussed the ways for providing more possibilities

for improving the security in IoT networks by integrating blockchain technology with the existing IoT networks. The decentralized and transparent behavior of the blockchain makes it more resilient with security and privacy in a peer to peer communication since most of the IoT applications are more distributed in nature which can compromise on the security and privacy. Thus blockchain when integrated with IoT networks will signi cantly address these concerns in the existing networks.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE communications surveys & tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in iot: The challenges, and a way forward," Journal of Network and Computer Applications, 2018.

[3] A. Colakovič and M. Hadialić, "Internet of things (iot): A review of enabling technologies, challenges, and open research issues," Computer Networks, vol. 144, pp. 17–39, 2018.

[4] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10–28, 2017.

[5] S. Balaji, K. Nathani, and R. Santhakumar, "Iot technology, applications and challenges: A contemporary survey," Wireless Personal Communications, vol. 108, no. 1, pp. 363–388, 2019.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] H. F. Atlam, R. J. Walters, and G. B. Wills, "Internet of nano things: Security issues and applications," in Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing. ACM, 2018, pp. 71–77.

[8] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017, pp. 618–623.

[9] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the iot and industrial iot: A review," Internet of Things, p. 100081, 2019.

[10] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[11] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," Sensors, vol. 18, no. 8, p. 2575, 2018.

[12] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," arXiv preprint arXiv:1608.05187, 2016.

[13] Y. Zhang and J. Wen, "The iot electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 983–994, 2017.

[14] M. Samaniego and R. Deters, "Blockchain as a service for iot," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2016, pp. 433–436.

[15] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy challenges," Internet of Things, p. 100107, 2019.

[16] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," Computer Communications, 2019.

[17] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "Iot information sharing security mechanism based on blockchain technology," Future Generation Computer Systems, vol. 101, pp. 1028–1040, 2019.

[18] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing iots in distributed blockchain: Analysis, requirements and open issues," Future Generation Computer Systems, vol. 100, pp. 325–343, 2019.

[19] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for iot security," Internet of Things, vol. 1, pp. 1–13, 2018.

[20] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5g-enabled iot for industrial automation: A systematic review, solutions, and challenges," Mechanical Systems and Signal Processing, vol. 135, p. 106382, 2020.

[21] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, "New blockchain-based architecture for service interoperations in internet of things," IEEE Transactions on Computational Social Systems, vol. 6, no. 4, pp. 739–748, 2019.

[22] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," Journal of Industrial Information Integration, vol. 13, pp. 32–39, 2019.

[23] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," IEEE Access, vol. 6, pp. 32 979–33 001, 2018.

[24] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," IEEE Communications Surveys & Tutorials, 2018.

[25] L. Da Xu and W. Viriyasitavat, "Application of blockchain in collaborative internet-of-things services," IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1295–1305, 2019.

[26] P. Urien, "Blockchain iot (biot): A new direction for solving internet of things security and trust issues," in 2018 3rd Cloudification of the Internet of Things (CIoT). IEEE, 2018, pp. 1–4.

[27] Gartner, Hype cycle for blockchain technologies, 2019. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-for-blockchain-busi

[28] H. F. Atlam and G. B. Wills, "Technical aspects of blockchain and iot," 2018.

[29] M. Ahmad and K. Salah, "Iot security: review, blockchain solutions, and open challenges, Futur. Gener. Comput. Syst. 82 (2018) vol. 82, no. 395, 2018.

[30] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Crypto- currency Technologies, 2016.

[31] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money," Banking Beyond Banks and Money, New Economic Windows, Springer, Cham, pp. 239–278., p. 239, 2016.

[32] R. Casado-Vara, J. Prieto, F. De la Prieta, and J. M. Corchado, "How blockchain improves the supply chain: Case study alimentary supply chain," Procedia computer science, vol. 134, pp. 393–398, 2018.

[33] S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.

[34] D.-S. WiKi, "accessed on march," 2016.

[35] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, 2018.

[36] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, "Blockchain-based business process management (BPM) framework for service composition in industry 4.0," Journal of Intelligent Manufacturing, 2018.

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

[38] C. Xu, K. Wang, G. Xu, P. Li, S. Guo, and J. Luo, "Making big data open in collaborative edges: A blockchain-based framework with reduced resource requirements," 2018 IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–6.

[39] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.

[40] X. Wang, G. Yu, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, K. Zheng, and X. Niu, "Capacity of blockchain based internet-of-things: testbed and analysis," Internet of Things, p. 100109, 2019.

[41] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software de ned fog node based distributed blockchain cloud architecture for IoT," IEEE Access, vol. 6, pp. 115–124, 2018.

[42] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," Wiley Online Library, vol. 10., Mar. 2018.

[43] G. Wood, ""ethereum: A secure decentralised generalised transaction ledger,"" Ethereum Project Yellow Paper, vol. 151, 2014.

[44] V. Dhillon, D. Metcalf, and M. Hooper, ""the hyperledger project, " in Blockchain Enabled Applications," p. 139–149, 2017.

[45] J. Fair eld, ""smart contracts," bitcoin bots, and consumer protection, " Washington and Lee Law Review Online, vol. 71, no. 2, p. 35–50, 2014.

[46] N. Atzei, M. Bartoletti, and T. Cimoli, ""a survey of attacks on ethereum smart contracts (sok)" in Proc. of the, vol. 6, p. 164–186, 2017.

[47] K. J. O'Dwyer and D. Malone, ""bitcoin mining and its energy footprint, " in 25 th IET Irish Signals Systems Conference and China- Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), Jun. 2014, p. 280–285.

[48] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," Ieee Access, vol. 4, pp. 2292–2303, 2016.

[49] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based iot systems: Integration issues, prospects, challenges, and future research directions," Future Generation Computer Systems, 2019.

[50] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019.

[51] I. Homoliak, S. Venugopalan, Q. Hum, and P. Szalachowski, "A security reference architecture for blockchains," 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, 2019, pp. 390–397.

[52] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trustchain: Trust management in blockchain and iot supported supply chains," in 2019 IEEE International Conference on Blockchain (Blockchain) IEEE, 2019, pp. 184–193.

[53] H. Desai, M. Kantarcioglu, and L. Kagal, "A hybrid blockchain architecture for privacy-enabled and accountable auctions," 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, 2019, pp. 34–43.

[54] . F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, ""fog computing and its role in the internet of things, " in Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, MCC," 2012, p. 13–16.

[55] A. Seitz, D. Henze, D. Miehle, B. Bruegge, J. Nickles, and M. Sauer, "Fog computing as enabler for blockchain-based iiot app marketplaces-a case study," 2018 Fifth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE, 2018, pp. 182–188.

[56] R. Brundo and R. De Nicola, "Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards," IEEE Communications Standards Magazine, vol. 2, no. 3, pp. 22–28, 2018.

[57] M. Li, L. Zhu, and X. Lin, "E cient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," IEEE Internet of Things Journal, 2018.

[58] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

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

[60] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to iot applications and beyond," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8114–8154, 2019.