Blockchain and IoT based revolutionized Technologies for making human Life styles smarter: BIoT Smart Technology

Dr. Savita Mohan, Dr. Meenu Sahni, Dr. Monica Srivastava
Department of Computer Science
GNIOT Institute of Professional Studies, Greater Noida
mnu.sahni@rediffmail.com

Currently, we are living in an era where we have little time for hard work. Two technologies have revolutionized our lives, benefiting and facilitating a smarter lifestyle. These technologies not only save time but also promote sustainability by automating electronics and electric devices, thus conserving electricity. Smart cities now rely heavily on the Internet of Things and blockchain technology. These technologies are interdependent; one cannot be fully implemented without the other. These advancements have fundamentally transformed the way we interact with our environment, paving the way for a more connected and efficient world. By harnessing the power of data and decentralization, these technologies enable us to create sustainable solutions for the challenges of today and tomorrow. As we continue to innovate and integrate these technologies, we stand on the brink of unprecedented possibilities in shaping our future. This chapter is dedicated to exploring these technologies and explaining their past, current, and future implications.

Keywords: Blockchain, Fog of Things (FoG), Cloud of Things (CoT), SDN, Point-to-Point (P2P), Machine-to-Machine (M2M), Ethereum, Security, Privacy, Immutability, Distributed Transaction Ledger (DTL).

Introduction

In modern world, there is an immense change in digitalization. Now the era has shown interest in **Interest of Things (IoT)** and its capacity for innovative features in various applications. The academicians, researches and entrepreneurs are blessed with the technology of **IoT.** Through **IoT** we interconnect heterogeneous devices for physical network which are automatically managed and controlled without human efforts. With the popularity of various industrial 4.0 based technologies, IoT is the field of opportunity and anticipation of worldwide people approx. 60 billion connected devices by 2024. The indispensable elements like **Cyber – Physical system (CPS), Wireless Sensor Networks (WSN)** and **Machine-to-Machine (M2M)** have been developed for the term **IOT.** Consequently, security is the more concern area with the development of IOT because through malicious attackers, **IoT** services can be endangered and for today's world data security and privacy are to be bothered for entire network confidentiality. We need to protect the entire network framework from the attackers, So that **IoT** with the standard network protocols become secured.

Furthermore, Blockchain (BC) has been successfully applied in Bitcoin for security and preserving privacy for IOT applications. With the elimination of centralized authority, the BC provides security and privacy for data storage, and its processing that reduces the risk of network attacks. Through in transactional database, BC reduces the frauds using the distributed network nodes. In present scenario, huge data transmission with IOT technology may occur poor Quality of Service (QoS). One failure may cause interruption in entire network system. For high QOS, reliability and availability, the quality assumes for data transmission, its security and privacy is must. The BC has all possible solutions to overcome from this problem where end to end user encrypted for IoT data.

However, blockchain significantly evolved decentralized applications. Its removes the centralized authorization in the verification stage, digital signatures for secured data, its architecture and privacy challenges. Blockchain intended to pursue a trust with independent users who do not rely on single third-party. In this manner blockchain create trust for a particular system, by increasing the degree of confidence between participants which also means that BC indirectly minimizing the need of trust. Since BC is open-source software where code of a specific task can be open the literature of outcomes can be easily predicted and by its architectural arrangements therefore user's trust and confidence can be achieved. Anyone can see the crypto currency protocols, where the software codes are highly predictable, user rely on technology and lesser the need of assurance of third party either developers or operators.

Further, challenges admissible while using blockchain with **IoT** is big issue. The complexity of blockchain, its higher computing cores, delays and handling data of **IoT** with blockchain has been discussed as :

Transparency and Privacy :

Blockchain can assure about transparency in financial transaction. However, user's reliability may be not sure while storing and accessing data from IOT technology on blockchain e.g. E-health. To manage the high degree of transparency and privacy, the reliability in cost-effective access control must be seen in IOT services using blockchain.

Regularize the challenges in blockchain with IoT :

Whenever we discuss the features of **BC** technology, we consider its decentralization, reliability, immutability, sustainability, automation and anonymity are key features for promising security solutions for diverse **IoT** services but these features may regulate new challenges. As we discussed about immutability,

the data is permanently stored in **Distributed Transaction Ledger (DTL)** in peer-to-peer networking and neither can be modified nor deleted. Also, as per the government policy, data can not be filtered and sorted for maintaining privacy before floating on blockchain. While code execution, if some interruption cause such as smart contracts on distributed transaction ledger then low can be breached. As per **DTL** anonymity, there is no straight method to distinguish the malicious users that pursuing illegal services from the genuine party. The feature like automation in blockchain has led to an advantage that code errors end obfuscating codes are ambiguous. The present laws of **IoT** and its regulations are now outdated especially when we

advent new technology as disruptive technology in blockchain. Now it's necessary to update it to undertake the **Distributed Transaction Ledger (DTL)**.

Big Data On Blockchain :

In the networking of blockchain, every user maintains a local record of the distributed ledger. Till the new block confirmation , the block is float throughout the entire network of peer-to-peer and each node appears the block confirmation for their local ledger. With the decentralized feature of blockchain, it solves the bottleneck problem and remove the requirement of technical system such as developers and operators. The structure improve the efficiency but management of **IoT** applications on blockchain can do maximum allocation on user's storage space. According to the study, blockchain node for 1000 participants need **730 GB** approximately in exchange of **2MB** single image/day in blockchain application. Therefore the challenge is to enhance the data storage capacity. While using **IoT** data on the blockchain.

Connectivity of IoT :

The **IOT** has limitations as limited capacity to connect but the actual expectations are high computing storage and maximum potential stakeholders to share big data with all networking resources. Through with limited capacity of blockchain, the blockchain provides best opportunities and services for the implementation of new applications in various domains.

Data Concurrency and Throughput Issue :

As we talk about **IoT** system, the continuously data streaming is there in **IoT** devices which shows high concurrency rate. And the throughput of blockchain is limited with complex security protocols of cryptography and consensus mechanisms. For the fast and continuous synchronization of new blocks among **BC** requires high bandwidth which can improve throughput of **BC**. This we face the challenge to boosting blockchain throughput so that the need of frequent transactions must meet in **IoT** systems.

Energy Consumption, Performance and Security:

The more electricity required for computation in running of blockchain algorithm which intend to slow down because of advancement of technology based applications on smart devices which are resource constrained. In crypto-currency, energy consumption is high as compared to domestic consumption of Ireland where **IoT** services cannot undertake current reports shown that entire crypto-currency absorbs high energy rather than some of the countries **E.g. Austria and Colombia**. Also, in recent study, researches may ask about the blockchain performance for the processing of **IoT** data and recommend (heat)* enhancement of blocks per second for the optimization of algorithm. To eliminate the blockchain **Proof Of Work (POW)** implies that consensus mechanism can minimize the energy consumption and enhance the performance of services. On the other hand, proof of work makes the blocks of blockchain tamper proof by the prevention of malicious and sybil attacks. Therefore, the target is to refine the processes of blockchain with regularize the alignment of security, privacy and efficiency. Now a days, researches are exploring about **IoT** data audits challenges for medical domain like supply-chain of medicines, pharmaceutical industry, e-health insurances, etc., digital signature in verification process and its safety, smart cities, farming and industrial revolution by blockchain

technology. Recent study mention about state-of-me- art work on **BC** in reference of **IoE (Internet Of Energy)** to provide users with a broad (spectrum)* into upcoming potential and its applications in digital sector. They elaborate about various applications related to blockchain, smart cities for power management **E.G**. Big data exchange automatically, power transactions, power demanding and business on secured blockchain end-to-end user connectivity. Further, we summarized that diverse technology of blockchain applications in **UAV (Unmanned Aerial Vehicles)** with in depth study show how blockchain help in finding **UAV** problems and resolving the issues. **UAV** describe as class of robotic machines that can move payloads and carry strike missions with autonomous control stations or remote control stations. But new challen ges arises **E.G**. air traffic increase, to establish the optimum routes, flight plans, energy management and **UAV** (swarms)* management and malicious attacks on **UAV**. Research explain that by the use of disruptive technologies like blockchain these issues can be reduced. Reviewers mentioned that through blockchain technology, industrial obstacles can be reduced so diverse industrial sectors opt the blockchain technology. Present main concern is security threats that can be identified by multiple cyber sources for **IoT** data with respect to different layers of **IoT** services. Further discussions can be made on various issues raised because of solution itself. How, sum up the major applications with technical details of blockchain in smart grid format and its prospects in commercial implementation. The challenges faced advancement of smart cities adopting blockchain technology. They suggested the **IoT** data an blockchain technology in the architecture smart agriculture. The researchers highlight the short comings of present and future research in the field of artificial intelligence. while blockchain adoption and its technologies in smart-grid explained in survey article. In survey article, latest research has been directed in this field. In literature review, analysing the security trends with the advancement of smart cities adopting blockchain technology. They suggested the IoT data an blockchain technology in the architecture smart agriculture. The researchers highlights the short comings of present and future research in the field of artificial intelligence.

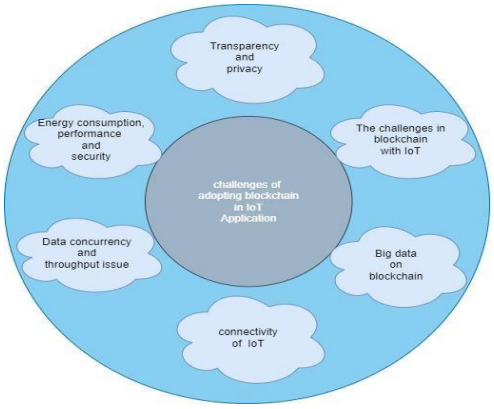

Fig. 1. The challenges of adopting blockchain in IoT(Internet of Things)

The purpose of this paper is to review the recent state of art work related to blockchain in different **IoT** services and discuss those tasks with regard to various blockchain technologies. Our research paper is different from existing research papers on **IoT** data with blockchain technology in many ways.

Most of the research papers review on adapting the blockchain technology for particular IOT stream. In contrast, we focused on state-of-art works in different **IoT** area including smart cities, e-health, e-insurance and smart agriculture.

In present survey papers, reviewers explained the present blockchain technology with limited services while we worked on various components of blockchain technology which breakdown the reviewed studies. Also, we detail the basic of blockchain technology for **IoT** data to influence maximum readers.

2. Our contribution in this paper has been mentioned as:-

Describe various components of blockchain as financial transactions, data transactions, verification and digitalization of signatures, number of blocks in blockchain, consensus mechanism, types of blockchain technology and its advantages VS limitations whenever consider with **IoT** area.

Analyse and review the latest paper of blockchain with regard to features like:

a) Utilization of different type of blockchain technology.
b) Application of consensus mechanism.
c) Implementation of access control mechanism.
d) Scalability and reliability.
e) Storage mechanism.
f) Utilization of stimulators.
g) Major outcomes and contributions in advancement of technology.
h) Short comings and remarks.

The challenges and gaps occur in research of contemplating blockchain into **IoT** area has been found and discussion on as much possible solutions are address in this literature review.

Table 1 : **The list of acronym**

Acronym	Definition	Acronym2	Definition3
ABE	Attribute-Based encription	LPoS	Leased proof of stake
ACL	access cntrol list	LSTM	long short term merory
AHS	artificial healthcare system	M2M	Machine-to-Machine
API	Application Programming Interface	MAS	Multi agent system
ARX	Add Rotate xor	NFV	Network function virtualization
AV	Autonomous vehchile	NOS	Network Operating system
BASN	Bboady Area Sensor Network	OBU	on board unit
BC	blockchain	P2P	Peer to Peer
BCCoT	blockchain and cloud of things	PCA	Patient centric agent
BCFoT	blockchain and fog of things	PKC	Public Key cryptography
BCIoT	blockchain and internet of things	PoA	proof of authority
BFT	byzantine fault tolerence	PoBT	Proof of block trade
CAT	Computed tomography	PoET	Proof of elapsed time
CH	cluster Head	PoS	proof of stake
CORE	Comman open research Emulator	PoW	Proof of work
CPS	Cyber-Physical Systems	QoS	Quality of service
CSP	Cloud Service Provider	RFID	Radio-frequency identification
DAG	Direct Acylic graph	RL	Read latency
DDoS	distribution denial of service	RPM	Remote patient monitoring
DPoS	delegated proof of stake	RSU	Roadside unit
DS	digital signature	SAT	Security Access token
DTL	Distriuted Transaction ledger	SC	Smart Contract
EMR	Electronic Medical Record	SDN	Software defined Network
EVM	Etherum virtual machine	SGX	Intel software guard Extention
G2V	grid to vehcile	SVM	Support vector Machine
GDPR	General data protection regulaton	SWF	Simple workflow service
HER	Electronic health record	TL	Transection letancy
HLF	Hyperledger Febric	TRL	Transaction and read latency
IoE	Internet of everything	TRT	Transaction and read throughput
IoE	Internet of energy	V2G	vehchile to grid
IoT	Internet of Things	VANET	vehicularDistributed Ad-hoc
IPFS	Interplanetry file system	VANET	Vehicular adhoc nrtwork
LoUT	Internet of underwater things	WSN	Wireless Sensor System

Here, Table 1 represents the acronym list used in this research paper. The paper is categorize in the following manner : initially we discuss about basics of blockchain. **Sections 1(a), 1(b), 1(c)** and **1(d)** elaborate the overview of fundamentals of blockchain technology,

the detailed study of blockchain technology, the purpose and limitations in this technology with **IoT** area respectively.

In the rest paper we discussed about potential adaptation of this technology in **IoT** services, **Fog of Things (FOT) , Cloud of Things(COT)** and technologies such as software defined networks are briefly defined in **2(a),2(b),2(c),** and **2(d)** respectively. The state-of-art examined the blockchain technology with **IoT** data, blockchain technology with **Fog of Things**, blockchain technology with **Cloud of Things** model in health sector, smart cities, smart vehicles network, supply chain, farming, industry and some miscellaneous **IoT** applications are presented in sections **3(a), 3(b), 3(c),** and **3(d)** respectively. The findings in research as gaps and solutions are explained in section (4)* and after that conclusion has been made in section (5)*.

3. Blockchain for IoT, FoT, CoT, and SDN Paradigm :-

In this section , we describe blockchain in detailed study as well as issues related to blockchain technology and **Internet of Things, Fog of Things, Cloud of Things** and software defined networks. The basics of blockchain technology are discussed in **section 2(a)** followed by detailed study of its each component in **section 2(b)**. in **section 2(c)**, the development of blockchain with **IoT** devices are described with some limitations. The study review in this section are **IoT, FOT** and **COT** with blockchain to design the framework for smart cities, agriculture, industry, **WSN(Wireless Sensor Network), e-health, etc.** The **Internet of Things, Fog of Things, Cloud of Things** and **SDN** together with blockchain are explained in **2.5, 2.6, 2.7** and **2.8** respectively after review the present research paper in different domains that amalgamate the technologies mentioned earlier.

Basis Of Blockchain :-

Blockchain can be defined as most trusted, secured, transparent and decentralized ledger for peer- to-peer network and known for its applications on crypto-currency introduced by **Mr. Santoshi Nakamoto**, 2008. The data transferred as unit in blockchain is said to be transaction and number of transactions are grouped in a block. The decentralized blockchain ledger has been developed because of confirmed blocks. In distributed ledger, the block is connected with previous approved block using block cryptographic hash code. This emerging technique has already been discussed to develop a variety of applications beyond digitalized cryptocurrency. Each and every user on a peer-to-peer network can easily verify the action of other users within the network and also make, verify and give approval for new transactions to be recorded in blockchain technology. This architecture ensures the secured, stable, transparent, and efficient blockchain operations with the goodness of tampering the resistance and minimizes the point of failure vulnerability. The blockchain ledger can be accessed by all participants but still not regularize by any kind of network authorities . the principle is obtained by following strict rules and mutual settlement among the network which is the feature of consensus mechanism. The consensus mechanism explains the process of synchronization in the decentralized ledger among all nodes in the **BC** network. Fig 2 represents an overview of Bitcoin blockchain operation.

Detailing Of Blockchain :-

In many research articles, the partitioned blockchain technology in different layers. The section confirms for five layer structure of blockchain along with the discussion of it's core properties related to reliability, transparency, security, privacy and integrity. The structure of blockchain in layered form can be depicted as :-

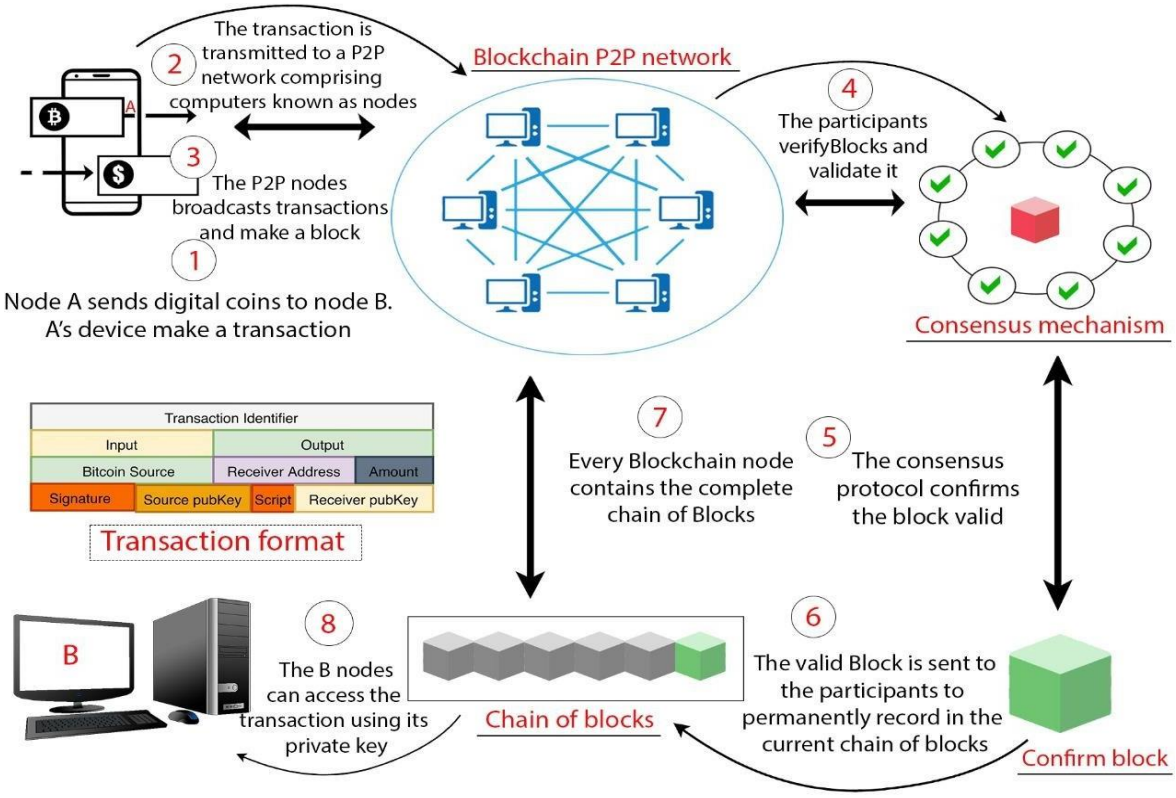

Fig. 2. The basic operation of Bitcoin blockchain (adopted from Ref. [35] with permission). P2P: peer to peer.

Here, the superscript in front of the bullet points is mapped to the different steps of Fig. 2.

① A participant A transfers a certain amount of digital coins to another participant B. A's device initiates a transaction. Participants can usually use their portable devices such as smartphone, laptop and low- processing computer for making transactions. The transactions are signed with A's private key and if necessary, the transaction contents are encrypted with B's public key.

② A's device transmits the transaction to a peer to peer network comprising of high-processing devices also called nodes. The blockchain protocols are implemented on this network.

③ The nodes on the blockchain network replicate the transaction and broadcast it throughout the network. The nodes packed a certain numbers of transactions in a Block. The structure of a typical Block is depicted in Fig. 4.

④⑤⑥ All the participants append the Block to existing chain of confirmed blocks only if a target hash code is created by solving complex mathematical puzzle known as Proof of Work. This process called

consensus mechanism varies in terms of computational cost and turnaround time. Some of the popular consensus mechanisms are discussed in the later section.

⑧ B's device can access the transaction from the confirmed Block using its private key.

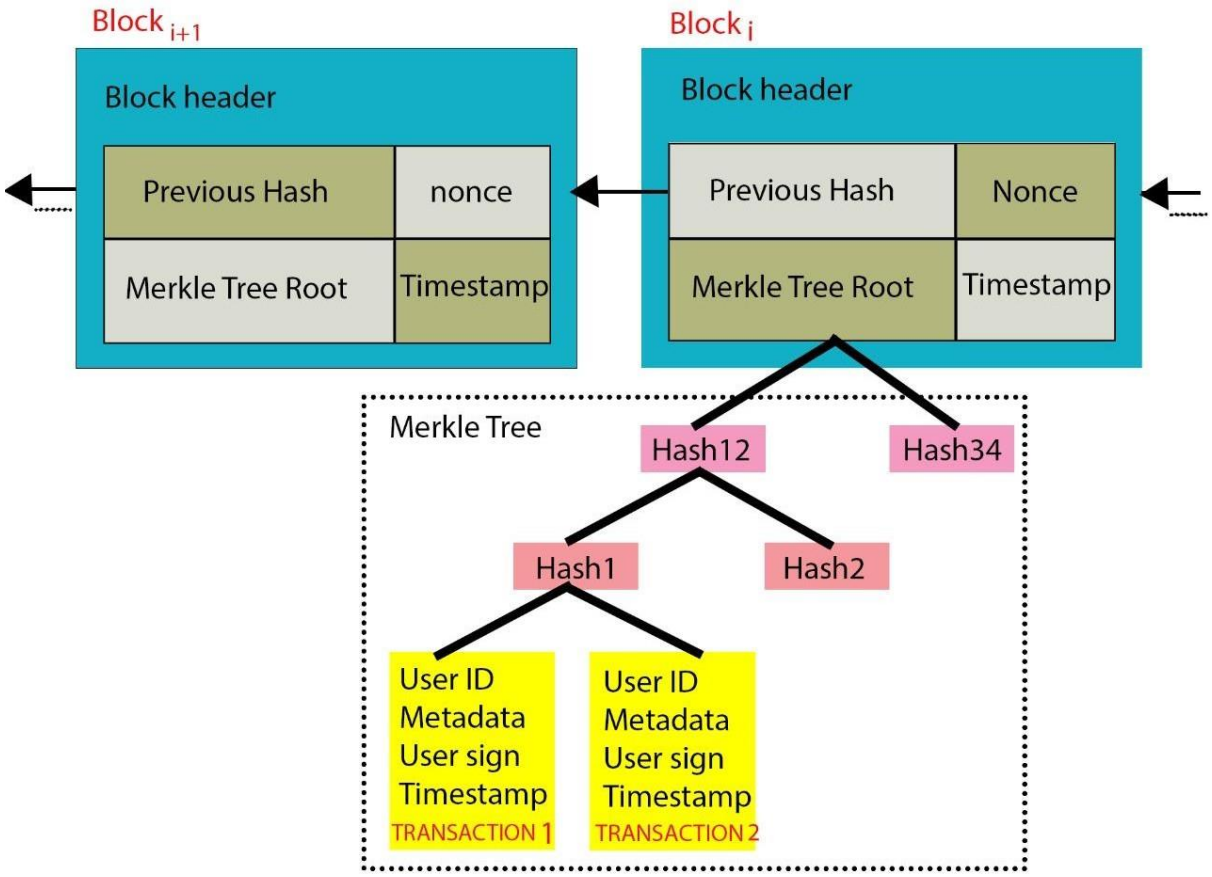

Fig.3. The bitcoin block header hashing algorithm (adopted from reference [40] with permission).

4. Types of Blockchain

Fig 3 represents the classification of **DTL**. The **DTL** is different from data structure and accessibility.

In chain architecture of **DTL**, blocks are interconnected in linear sequential form while graph-structured **DTL** saves transaction in a **DAG(Distributed Acyclic Graph).** Single **DAG** transaction is directly linked with each other rather than jointly connected and processing is done in blocks. As per accessibility, blockchain technology can be distributed in two major categories: public (permission-less) and private (permitted). The public blockchain technology represents non- restricted behaviour, permission less **DTL** that permits everyone to join the network for transactions and engage in consensus process. In public blockchain, bitcoin and ethereum are open source and smart contracts. Public blockchains are sustainable and reliable if the users follows the strict norms of blockchain.

On the other side, the private blockchain is the invite network authorised by central authority and in validation process, users are allowed to confirm the transaction in the **BC.**

Further, a blockchain developer team argue that private blockchain cannot be bothered as blockchain because monitoring, privacy, tracking, security and restriction are the principles of private blockchain that contradicts the trust and open source of blockchain. In both chains either private or public, many features are different. In public blockchain, validators are unlimited so not trustworthy whereas in private blockchain, premediated validators results higher throughput and strong privacy in its distributed ledger. Transaction through public blockchain is tamper-proof and can never be modified but in private blockchain, a committed transaction can be modified and updated follow the consensus mechanism for a certain number of authorized users.

To set a network, no infrastructure costs required by public blockchain but operational cost and development cost needed in wide-scale private blockchain technology. Rimba et al. [120]* gives the comprehensive study for computation cost and storage cost of a blockchain in cloud. They run two business process for two different kinds of architecture: Ethereum and Amazon SWF(Amazon Workflow Services) to propose estimate casting for the business process logic. Rimba et al [120]* comparing the execution cost of Ethereum blockchain is two order greater than Amazon Simple Workflow Services.

Other blockchain type is consortium, a semi-decentralized and governed by group of people rather than individual. Various blockchain are used in this research article given in [Table 5].

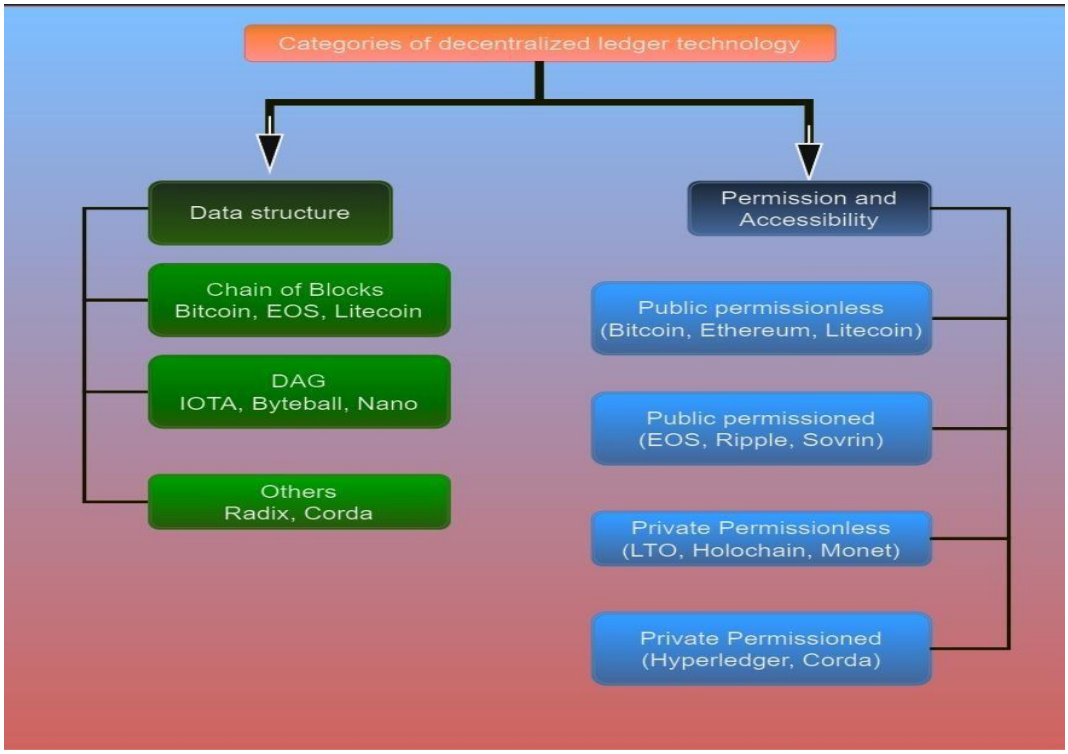

Fig. 4. the types of decentralized ledger technology. DAG: distributed acyclic graph.

5. Sidechain :

The sidechain [121] defines as separate blockchain which operates parallel to the main blockchain and both chains are attached by two-way peg. The main chain is also called parent or original chain and all connected chains are refer to as side chain. The two-way peg has been depicted in [fig.12]* and it follows bidirectional transfer mechanism where users move their digital transaction to the side chain from the original blockchain and vice-versa. The user send a certain amount of digital coin on the main blockchain from the outside address of a system called Federations. After a certain time of transaction of digital coin committed by user, the Federation releases equivalent coin in the side blockchain. The participant then access and spend the digital currency on side blockchain. The reverse process also occurs from side blockchain to the main blockchain. The Federation is an intermediator of side chain and primary chain to determine the locking and unlocking of digital coins. The Federation also work as an extra layer between the side blockchain and main blockchain. The selection of the members of the federation is done by developers of the side blockchain. The side blockchain has own protocols and implementation rules for smooth running and is independent from the main blockchain.

Table 2 : Different types of blockchain in IoT literature.

Acronym	Explanation	Interpretation
CB	Cloud blockchain	Third-party cloud such as AWS provides resource for buildings and operating blockchain operation.
CoB	Consortium blockchain	The consortium blockchain is a semi private which is controlled by a group of user across different organisation.
CuB/CPuB/CPrB	Customized blockchain/customized Public blockchain/customized Private blockchain	Developers or researchers use popular programming language like c++, java, python, go language to build their own private or public blockchain for analyzing the performance of their applications.
EEB	Enterprises ethereum blockchain	Ethereum is the second-largest enterprises open-source blockchain which is used for general purpose.ethereum facilitates smart contract and disribute application(dApps) to build and run without the the requirements of third party,any fraud amd downtime.
EHF	Enterprise hyperledger febric	Hyperledger febric refers to an open-source, permissioned distributed ledger developed by the linux foundation hosted Hyperledger consortium. The clint application use hyperledger fabric SDK or REST Web service to interect with hyperledger febric network.
EPB	Enterprise permission blockchain	This is industry level blockchain such as Hyperledger fabric where user require permission to participate in the network.
PrB	Private blockchain	The private blockchain allows only trusted parties to participate in the network to verify and validate transaction.
PrEB	Private ethereum blockchain	Ethereum blockchain networkdescribr a set of nodes connected to each other to creat a network. Developers can build a private Ethereum network rather then public network to make transactions and build a smart contract without the need of real Ether.
PrPB	Private Permissioned blockchain	This blockchain is permissioned and private ,so only selected participents can join the network . (e.g., Hyperledger Fabric, R3's Corda).
PuB	Public blockchain	Each of transaction in a public blockchain is open for public to verify.Anyone can download blockchain protocols and read, write or participate in the network.
PuPB	Public permissioned blockchain	A Public permissioned blockchain network is defined as new kind of network that bridges the gap between the public permissionless network (such as Bitcoin or Ethereum) and the private consortium network.

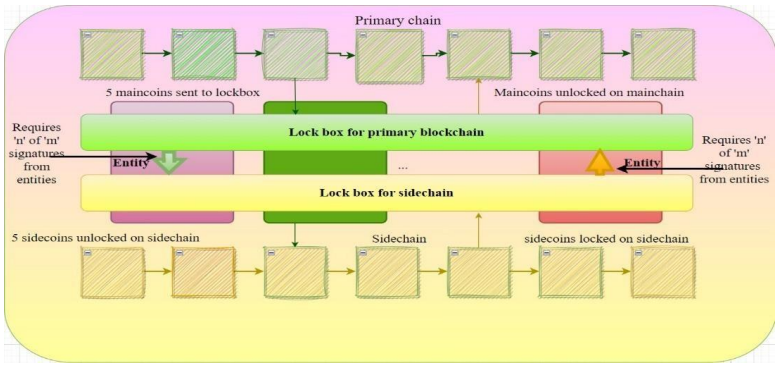

Fig. 5. The federated two-way peg communication.

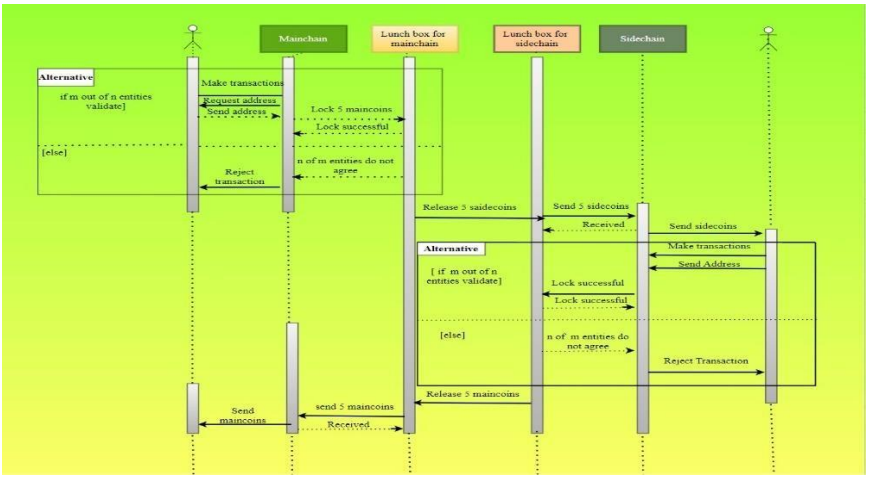

Fig. 6. The sequence diagram of two-way peg communication.

As a result, the malicious attacks on main blockchain cannot compromise the side blockchain and side chain can still operating likewise the hacked side blockchain can not affect the operations of main blockchain.

The sequence of communication between main blockchain, the Federation and side blockchain can be represented by a diagram as (Fig.6) where:

1. A participant transact 5 main coins to the Federation, that locking the coin and the coin not transfer to the side blockchain.
2. After performing verification, the federation sign the transactional entities. The number of entities approved for the transaction are then received the 5 main coins that transferred by the user and address provided on the side blockchain.
3. If users are playing any game and each have 5 side coins then the winner got 5+5 side coins i.e. total 10 side coins. Also, if game is drawn then each participant have its original side coins i.e. 5 side coins each.
4. The participant send back side coins i.e. originally they have 5 side coins to the lock box of the Federation. Again, the Federation entities verifies the transaction and send back the coins to the main chain.

6. Performance metrics of Blockchain Application:

In today's scenario, different type of blockchain based applications are working. So, it is necessary to see the performance, success and limitations of blockchain

technology in various developing use case. Fan et al [48] conducted a survey based on blockchain (metrics)* tools and performance assessment parameters. The three tools presented in (table3), Hyperledger caliper,

blockbench and DAG-bench highlighted by Fan et al [48] , analysing the performance of both blockchain technology viz. private blockchain technology and public blockchain technology on the basis of two

stimulators like DAGSim and blockSim, under the category of blockchain benchmarks tools. Studies [39, 122-124] reviewed the parameters for assessing **Decentralized Transaction Ledger (DTL)** and

performance set metrices blockchain technology leveraged by IoT applications as mentioned in [Fig.7].

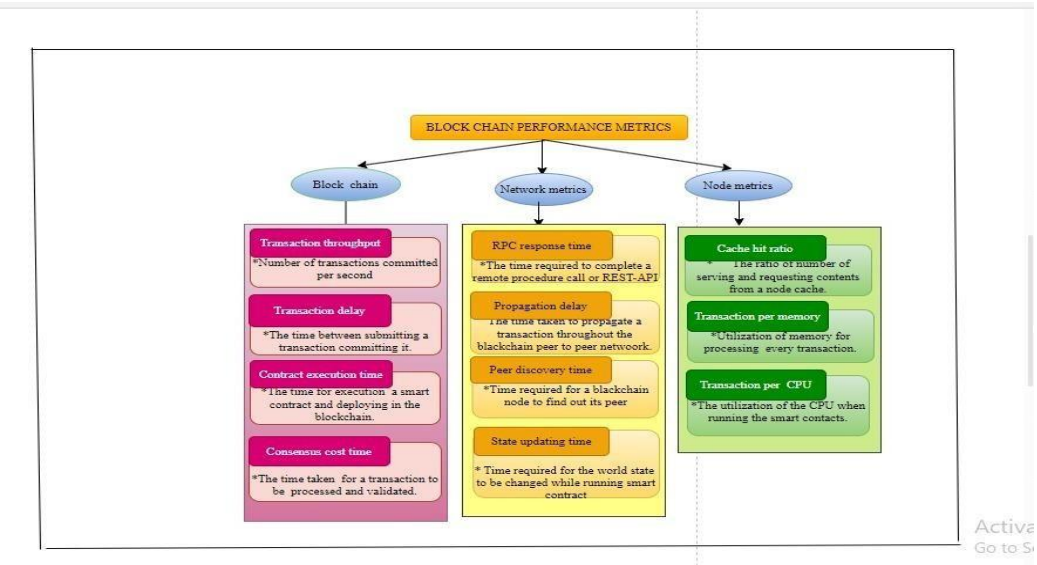

Fig. 7. The metrics for evaluating blockchain leveraged applications.

Table 3
Performance metrics for different blockchain

Tool	Performance Metric	Supported blockchain
Blockbench [**125**]	Throughput, Latency, Scalability and fault -tolerance	Ethereum, Party [**126**], HLF [**127**] andQuorum [**128**].
Blockchain simulator	block creation rate, system stability and transaction	Any private blockchain comparison with bitcoin,
Blockskim [136], blockSIM [**137**]	throughput (TPS)	Ethereum
DAGbench [**133**]	Throughput, latency, Scalability, success indicator,	IOTA[**134**], Nano, Byteball [**135**]
	resource consumption, transaction data size and	
	transaction fee.	
DAGsim [**138**]	Transaction arival rate	IOTA Triangle [**139**]
Hyperledger Caliper [**129**]	TPS (Transaction per second), Transection latency,	Hyperledger fabric,sawtooth [**130**], Iroha [**131**],
	resource, utilization (CPU, RAM, Network, and IO).	Burrow [**132**] and Besu.

7. Objectives of blockchain in IoT :-

The advent of blockchain has many features across a variety of many industries in trustless scenario [44]. In this section, various merits and objectives of the blockchain technology in IoT in [Fig.8] has been described.

Decentralization :-

Blockchain technology is a promising technique with its decentralized nature, for effectively solving bottleneck and single-point failure issues by removing the requirement for a trusted third party in **IoT** services [8]. The blockchain node disruption does not affect any of the operation of blockchain and **IoT** network . In blockchain technology , data is stored in multiple nodes of peer-to-peer network and the system is highly resistant proof for any malicious attacks and technological failures . The security and privacy of the network can not be taken as granted even if some nodes are in offline mode. On the other side, some traditional database depend upon one or more servers and therefore prone to technological failure and cyber attacks . Furthermore , the **p2p** structure of blockchains strengthen all network attendees with fair validity to verify the rightness of **IoT** data and ensures immutability.

Enhanced Security :-

Blockchain is sustainable , reliable , security and ensures privacy then other record maintaining application from all aspects [8]. Transactions are agreed in prior basis for being documenting by and users. The transaction is first encrypted and then linked to the prior transactions after approval . Also , information is stored across the network rather than one server, through which data can not be compromised from hackers. In blockchain, the key feature of security is public and private key **(PKI)**. The keys are generated with random strings and keys so that no one can formulate the private key from the public key.

This type of system in blockchain between users are known as a symmetrical cryptography . This technique reduces data leakage problems, future attacks and gives strength to the blockchain network.

Moreover highly protective and sensitive data in different sectors need confidentiality from frauds and illegal activities because the data is stored for various applications E.G. in financial sector , government sector , and health sector are important service areas . In addition , blockchain has smart contracts . Fraud -access verified and disabled by smart contract based authorisation.

Improved Traceability :-

Trading of goods complex chain use traditional ledger in which no one can trace the point of origin without verify the authenticity. Similarly, **BC** store and track past activities of all users . Previous data in **BC** can help in verifying the validity of assets and avoid fraud activities.

Greater Transparency :-

The greater transparency exists because history available for all network users rather than conventional network. Here, participants share the common documents not individual copy in standard network . The shared document edited or modified only by consensus of everyone . This leads to generate credibility of **BC** based system by overcome the problem of unauthorized data modification.

Data Privacy :-

Immutability and trustworthy are the extremely efficient feature of **BC** that protect **IoT** data from modification [18]. Blockchain archives events by preservation of integrity and guarantees authenticity by hash chains and digital signatory. Specially, **BC** permits users to monitor the data rights and transactions are retained across the computer network.

Reduced Cost :-

Blockchain follows cost reducibility by unchangeable ledger, no paper work for users to complete the transaction, escape the costing of third-party services because **BC** does not require middleman or third-party. Also, huge investment are required for private and consortium **BC** and certain changes for public **BC** E.G. Gas is Ethereum .

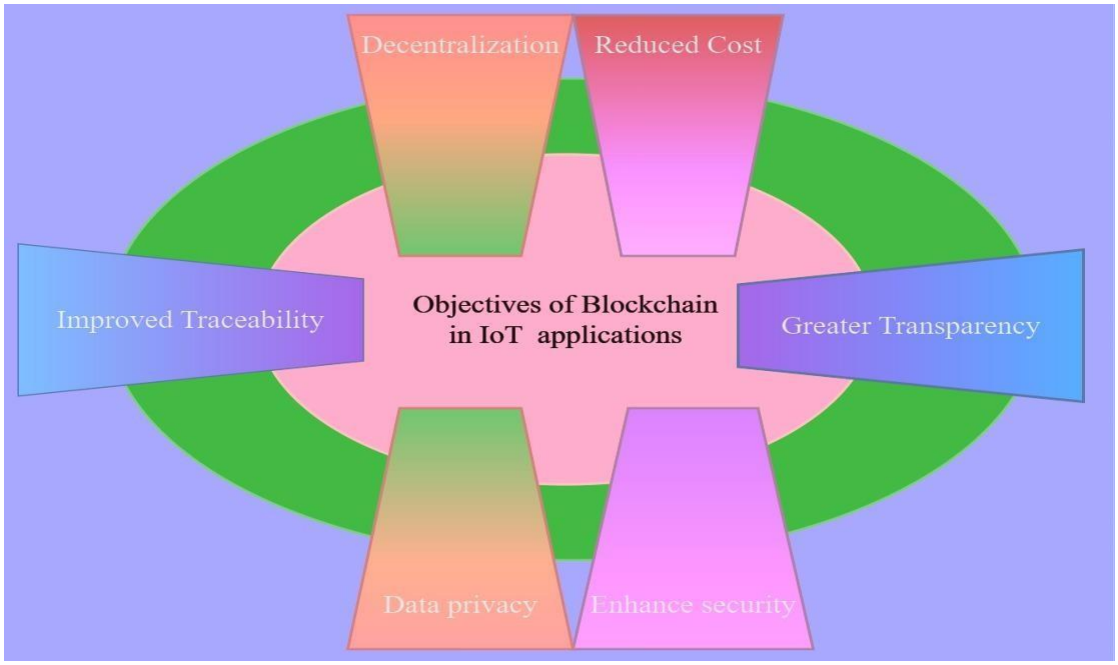

Fig. 8. The objectives of blockchain. IoT: Internet of Things

Immutability :-

Strong immutability preserves by hashing technique. By hashing, blocks linked together to form sequential chain. A field of new block's header has hash value of metadata of previous block. This way, data in blocks can not be changed, alterned, modified, removed or updated without validating in **BC**. With the help of cryptographic link, it changes occur then easily identified

8. Limitations of BC:

while BC has committed disrupting infrastructure for IoT services, its execution in series call some critical challenges that are discussed below : .

8.1 Scalability Limitations :-

Constraints in block size.
Block time increases fastly.
Complex IoT environment.

.8.1.4. Data complication with processing of high volumes.

Because of above mentioned lackness, developers not able to see BC technology because alternative series and solutions exist for large IoT systems[43].

High consumption cost : High running cost involves the processing like mining of data, validation , storing, and security for multiple participants . Various mining involves POW, PBFT, and POS in which consumption of high level of energy. **BC** sophisticated architecture demand high technical resources and human resources . This would trigger high running cost for implementation of large scale **BC** based systems.

Security And Privacy Issue :-

Message Hijack.

DDOS Attacks [32].

These attacks disrupt the mining process , financial services crypto exchanges and e- wallets, E.G. all genres of health care data causes a delay in committing transactions, data leakage risks and disclosure of sensitive patient's information.

9.The reviewed literature of BC and IoT

BC state-of-art applications in **IoT** are as follows:-

A. State-of-art works of **BC** in E-Health :-

- **BC** for hospital and drug management.
- **BC** for privacy preserving in E-Health.
- **BC** for M-Health.
- **BC** for access control in E-Health.
- **BC** leveraged storage for E-Health data.
- **BC** enabled data sharing in E-Health
- . **BC** smart contract in E-Health.
- Lightweight **BC** in E-Health
- . **BC** leveraged searchable encryption in E-health.
- . **BC** enable E-Health architecture.

BC in smart cities/homes.

BC with **IoT** vehicular network.

BC with miscellaneous **IoTs** :-

- Agent managed **BC** in **IoT**
- .**BC** for **SDN** enabled **IoT**
- .**BC** for securing **SDN IoT**
- .**BC** for mobile **IoT**
- .**BC** for wireless sensor networks
- .**BC** for **IoT** supply chain
- .**BC** based authentication for **IoT**
- .**BC** for **IoT** trust management
- .**BC** for **IoT** payment management.

BC with **IoT** ensures :-

- Balance between power consumption, performance and security.
- Balance between data concurrency and throughput.
- Address connectivity challenges.
- Handling big data on the **BC**.
- Maintaining both transparency and privacy.
- Address **BC** regulation challenges in **IoT**.

10. Challenges

Table : 4

The challenges and its solutions

SL No.	Challenges	Prospective Solution
1	Accommodation of huge volume of IoT data inblockchain	Many researches have suggested off-chain strategies to handle big data in IoT where conventional Cloud storage is integrated with blockchain storage. To deal with IoT big data, another approach is to distribute IoT data across multiple repositories including different Cloud service providing repositories, local computer, and on-chain of blockchain based on the characteristics and diverse contexts of the data [35,281].
2	Challenges of maintaining privacy in blockchain	Homomorphic encryption [282] and proxy re-encryption technique [245] have been investigated by several studies of blockchain and IoT to resolve the issue of user's privacy on the blockchain network. In addition, Federated learning [283] can be integrated with blockchain technology to ensure the privacy-preserving computation on users' data. Federated learning allows a machine-learning algorithm to be trained by the participants of the blockchain without exchanging their data where the blockchain can guarantee the security of the trained algorithm in the form of a smart contract.
3	Challenges of regulating IoT blockchain	Lessig [284] described four means: law, social norms, and economic means for governing any applications on the cyberspace. However, no effective legislation has yet been put in place to govern the existing blockchain-based IoT applications. Blockchain oriented IoT applications can be effectively regulated by combining the technology of four means proposed by Lessig. The integration of the autonomous agent with blockchain can assist in defining social norms and enacting law for regulating blockchain.
4	Connectivity challenges of IoT with blockchain	Sidechain [121] is a distinct blockchain that operates parallel to any enterprise public or private blockchain also called mainchain. To address the connectivity issue of IoT with blockchain, the MEC (Multi-access Edge Computing) can host sidechain which is close to the IoT network and enables the IoT devices to communicate with mainchain via the sidechain. Consequently, IoT devices can interact with the sidechain on the Edge network using their low bandwidth.
5	Higher bandwidth consumption in blockchain	Sharding [75] is a method of splitting blockchain peer to peer network into the different clusters. The members of a sharding are responsible for processing and verifying transactions generated in that sharding. This results in avoiding the propagation of a transaction across the entire network and hence can save bandwidth. An Edge-based personalized Agent can be appointed for each sharding where the agent collects transactions from IoT devices and make blocks to further reduce high bandwidth requirements of the blockchain.
6	Resource limitations of IoT to accommodate blockchain technology	Researchers [47,280] have suggested smart Agent or Gateway converge IoT devices with blockchain where the smart Agent performs computations, provide network and storage resources required to accommodate blockchain on behalf of IoT devices. Other kinds of solutions include 1) optimization of blockchain's algorithms including consensus protocol, security protocol 2) DAG-based blockchain [235] technology that can obviate the need of miners 3) Sharding that refers to partition of blockchain network [75].

11 .CONCLUSION :

We reviewed may research papers in several domains which includes **Internet of Things** in e-health, smart cities, business, vehicular applications which incorporated with Edge, **Fog, Cot, SDN** and **BC** technology to focus privacy and security issues. Nonetheless, various technologies and security arears remains unaddressed. In this paper, many challenges has been undertake **BC** in **IoT** domain are recognise and discuss. Existing BC with IoT are scrutinized with regard to different environment for

publishing their limitations and strengths. Furthermore, the paper includes a wide detailing of BC components and consensus mechanism.

12. DECLARATION:-

The authors stated that they have no financial interests, personal relationships and competing that may have appeared to enforce the work recorded in this paper.

References

1) S. Hassan, P. de Filippi, The expansion of algorithmic governance: from code is law to law is code, Field Actions Sci. Rep. 17 (2017) 88–90. Special Issue.
2) Z.J. Bao, W.B. Shi, D.B. He, et al., IoTchain: a three- tier blockchain-based IoT security architecture, arXiv, 2018. preprint.
3) A.S. Hosen, S. Singh, P.K. Sharma, et al., Blockchain-based transaction validation protocol for a secure distributed IoT network, IEEE Access 8 (2020) 117266–117277.
4) B.L.R. Stojkoska, K.V. Trivodaliev, A review of internet of things for smart home: challenges and solutions, J. Clean. Prod. 140 (2017) 1454–1464.
5) L. Marelli, E. Lievevrouw, I. van Hoyweghen, Fit for purpose? The GDPR and the governance of European digital health, Pol. Stud. 41 (5) (2020)
447–467.
6) H. Jin, Y. Luo, P.L. Li, et al., A review of secure and privacy-preserving medical data sharing, IEEE Access 7 (2019) 61656–61669.
7) P. Kochovski, S. Gec, V. Stankovski, et al., Trust management in a blockchain based fog computing platform with trustless smart oracles, Future Generat. Comput. Syst. 101 (2019) 747–
759.
8) F. Jamil, S. Ahmad, N. Iqbal, et al., Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals, Sensors 20 (8) (2020)
2195.
9) D. Boneh, Aggregate signatures, in: H.C.A. van Tilborg, S. Jajodia (Eds.), Encyclopedia of Cryptography and Security, Springer, Boston, MA, USA, 2011, 27–27.
10) D.C. Nguyen, P.N. Pathirana, M. Ding, et al., Integration of Blockchain and Cloud of Things:
Architecture, Applications and Challenges, arXiv, 2019. preprint.
11) K. Qayumi, Multi-agent based intelligence generation from very large datasets, in: 2015 IEEE International Conference on Cloud Engineering, IEEE, Tempe, AZ, USA. Piscataway, NJ, USA, 2015,
pp. 502–504, 9–13 Mar 2015.
12) P.Y. Zhang, F.L. Liu, N. Kumar, et al., Information classification strategy for blockchain-based secure SDN in IoT scenario, in: IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops; 6–9 Jul 2020; Toronto, ON, Canada, IEEE, Piscataway, NJ, USA, 2020, pp. 1081–1086.
13) Dorri, S.S. Kanhere, R. Jurdak, et al., Blockchain for IoT security and privacy: the case study of a smart home, in: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops; 13–17 Mar 2017; Kona, HI, USA, IEEE, Piscataway, NJ, USA, 2017, pp. 618–623.
14) X.G. Liu, Z.Q. Wang, C.H. Jin, et al., A blockchain- based medical data sharing and protection scheme, IEEE Access 7 (2019) 118943–118953.

15) L.J. Fan, J.R. Gil-Garcia, D. Werthmuller, et al., Investigating blockchain as a data management tool for IoT devices in smart city initiatives, in: 19th Annual International Conference on Digital Government Research: Governance in the Data Age; 30 May–1 Jun 2018; Delft, The Netherlands, ACM, New York, NY, USA, 2018, pp. 1–2.
16) Singh, K. Click, R.M. Parizi, et al., Sidechain technologies in blockchain networks: an examination and state-of-the-art review, J. Netw. Comput. Appl. 149 (2020) 102471.
17) Q. Xia, E.B. Sifah, K.O. Asamoah, et al., Medshare: trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767.
18) K. Huang, X.S. Zhang, Y. Mu, et al., Scalable and redactable blockchain with update and anonymity, Inf. Sci. 546 (2021) 25–41.
19) M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges, Future Generat. Comput. Syst. 82 (2018) 395–411.
20) Norta, A.B. Othman, K. Taveter, Conflict-resolution lifecycles for governed decentralized autonomous organization collaboration, in: 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia; 24–25 Nov 2015; St. Petersburg, Russia, ACM, New York, NY, USA, 2015, pp. 244–257
21) Z. Abou El Houda, A. Hafid, L. Khoukhi, Co-IoT: a collaborative DDOS mitigation scheme in IoT environment based on blockchain using SDN, in: 2019 IEEE Global Communications Conference; 9– 13 Dec 2019; Waikoloa, USA, IEEE, Piscataway, NJ, USA, 2019, pp. 1–6.
22) P.K. Singh, R. Singh, S.K. Nandi, et al., Managing smart home appliances with proof of authority and blockchain, in: International Conference on Innovations for Community Services; 24–26 Jun 2019; Wolfsburg, Germany, Springer, Cham, France, 2019, pp. 221–232.
23) Z. Kavosi, H. Rahimi, S. Khanian, et al., Factors influencing decision making for healthcare services outsourcing: a review and delphi study, Med. J. Islam. Repub. Iran 32 (2018) 56.
24) S. Schaller, D. Hood, Software defined networking architecture standardization, Comput. Stand. Interfac. 54 (2017) 197–202.
25) T.T.A. Dinh, J. Wang, G. Chen, et al., Blockbench: a framework for analyzing private blockchains, in: 2017 ACM International Conference on Management of Datal; 14–19 May 2017; Chicago, IL, USA, ACM, New York, NY, USA, 2017, pp. 1085– 1100.
26) Al Omar, M.Z.A. Bhuiyan, A. Basu, et al., Privacy- friendly platform for healthcare data in cloud based on blockchain environment, Future Generat. Comput. Syst. 95 (2019) 511–521.
27) C.Y. Li, Y. Tian, X. Chen, et al., An efficient anti- quantum lattice-based blind signature for blockchain-enabled systems, Inf. Sci. 546 (2020) 253–264.
28) R.A. Michelin, A. Dorri, M. Steger, et al., Speedychain: a framework for decoupling data from blockchain for smart cities, in: 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services; 5–7 Nov 2018; New York, NY, USA, ACM, New York, NY, USA, 2018, pp. 145–154.

29) M.A. Uddin, A. Stranieri, I. Gondal, et al., Dynamically recommending repositories for health data: a machine learning model, in: Australasian Computer Science Week Multiconference; 4–6 Feb 2020; Melbourne, Australia, ACM, cNew York, NY, USA, 2020, pp. 1– 10.
30) P.P. Ray, D. Dash, K. Salah, et al., Blockchain for IoT- based healthcare: background, consensus, platforms, and use cases, IEEE Syst. J. 15 (1) (2020) 85–94.
31) W.D. Tang, X. Zhao, W. Rafique, et al., A blockchain- based offloading approach in fog computing environment, in: 2018 IEEE International Conferences on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications; 11–13 Dec 2018; Melbourne, Australia, IEEE, Piscataway, NJ, USA, 2018, pp. 308–315.
32) S. Nadeem, M. Rizwan, F. Ahmad, et al., Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture, Int. J. Adv. Comput. Sci. Appl. 10 (1) (2019) 288–295.
33) C.F. Chou, W.C. Cheng, L. Golubchik, Performance study of online batch-based digital signature schemes, J. Netw. Comput. Appl. 33 (2) (2010) 98–114.
34) M. Li, J. Weng, A.J. Yang, et al., Crowdbc: a blockchain-based decentralized framework for crowdsourcing, IEEE Trans. Parallel Distr. Syst.30(6) (2018) 1251–1266.
35) M. Ho€lbl, M. Kompara, A. Kamisali¢, et al., A systematic review of the use of blockchain in healthcare, Symmetry 10 (10) (2018) 470.
36) H. Caliper, Hyperledger Caliper Architecture, 2019. Available online, https://h yperledger.github.io/caliper/docs/2_Architecture. html. (Accessed 3 October 2019).
37) E.Y. Daraghmi, Y.A. Daraghmi, S.M. Yuan, Medchain: a design of blockchain- based system for medical records access and permissions management, IEEE Access 7 (2019) 164595–164613.
38) M.A. Uddin, A. Stranieri, I. Gondal, et al., An efficient selective miner consensus protocol in blockchain oriented IoT smart monitoring, in: 2019 IEEE International Conference on Industrial Technology; 13–15 Feb 2019; Melbourne, Australia. Piscataway, IEEE, NJ, USA, 2019, pp. 1135–1142.
39) Z.Y. Wang, H. Yu, Z.Y. Zhang, et al., ECDSA weak randomness in bitcoin, Future Generat. Comput. Syst. 102 (2020) 507–513.
40) M.A. Rahman, M.M. Rashid, M.S. Hossain, et al., Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city, IEEE Access 7 (2019) 18611–18621.
41) N.L. Hickson-Brown, Prototyping und evaluierung des hyperledger burrow frameworks unter gesichtspunkten der usability, Ph.D. Dissertation, Universit€at Hamburg, Hamburg, Germany, 2019.
42) Hyperledger Caliper. Github, 2020. Available online, https://github.com/hyperle dger/caliper. (Accessed 15 June 2020).
43) L. Ismail, H. Materwala, S. Zeadally, Lightweight blockchain for healthcare, IEEE Access 7 (2019) 149935–149951.

44) H.F. Atlam, A. Alenezi, M.O. Alassafi, et al., Blockchain with internet of things: benefits, challenges, and future directions, Int. J. Intell. Syst. Appl. 10 (6) (2018) 40–48.
Y. Gao, Y.J. Chen, H.L. Lin, et al., Blockchain
45) basedsecure IoT data sharing framework for sdn- enabled smart communities, in: IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops; 6–9 Jul 2020; Toronto, ON, Canada, IEEE, Piscataway
, NJ, USA, 2020, pp. 514–519.

46) M. Li, L.H. Zhu , X.D. Lin, Efficient and privacy - preserving carpooling using blockchain - assisted vehicular fog computing, IEEE Internet of Things J. 6 (3) (2018) 4573–4584.
47) D. Calvaresi, V. Mattioli, A. Dubovitskaya, et al.,Reputation management in multi-agentsystems using permissioned blockchain technology, in: 2018 IEEE/WIC/ ACM International Conference on Web Intelligence; 3–6 Dec 2018; Santiago,
48) M . Li , L.H. Zhu , X.D. Lin , Efficient and privacy - preserving carpooling using blockchain -assisted vehicular fog computing , IEEE Internet of Things J. 6 (3) (2018) 4573–4584.
49) D. Calvaresi , V. Mattioli , A. Dubovitskaya , et al., Reputation management in multi - agentsystem
using permissioned blockchain technology , in: 2018 IEEE/WIC/ ACM International Conference on Web Intelligence; 3–6 Dec 2018; Santiago.