A Systematic Literature Review: Blockchain Based Solutions for IoT's

SHOAIB UL HASSAN, JINGXIA CHEN, MUHAMMAD AFRASAYAB

ALI AKBAR, MUHAMMAD AHSAN, TARIQ MAHMOOD

Department of Electronic Information and Artificial Intelligence
, Shaanxi University of Science and Technology
Xi'an, China
Department of Computer Science,
Govt. College University
Faisalabad, Pakistan
Department of Computer Science and IT,
University of Sargodha
Bhakkar, Pakistan

DOI: 10.29322/IJSRP.10.11.2020.p10765
http://dx.doi.org/10.29322/IJSRP.10.11.2020.p10765

***Abstract*--In the modern era, Internet of things brought revolution in the everyday life activities by automation in everyday functions, modifying the approach of people to collaborate with one another or with the devices. Actually, the main feature of IoTs is direct device to device interrelationship. Their benefits range from little domestic devices to heavy industrial systems. Despite of numerous advantages of IoTs, their execution contains different issues mostly due to the severe substance of the functions by implement and because of their narrow computing abilities. Blockchain is the forthcoming annoying technology field that has achieved the attention of IoT sectors to tackle the problems by becoming encountered by themselves. In the article, the relevant issues in IoT field are pointed by us and then examined by the method how these issues can be resolved with the help of Blockchain features. Furthermore, we have also identified issues that appear while allocation of blockchain (BC) in Internet of things (IoTs).**

***Keywords*--Internet of Things(IoT); Blockchain**

1. INTRODUCTION

In modern world technologies have great impact on the life standard of humans. This revolution is for advancement in intercommunication and invention of semi-conductor materials that allow gadgets to affiliate through a network and change the path of communication among electronic devices and human beings[8]. This phenomenon is commonly termed as Internet of Things (IoT). K. Ashton was the first person who invented the term IoT in 1999. In IoT, things around us are connected to the network. These things communicate and share their information with human and also with each other by the help of sensors which are installed in it. Internet of Things (IoT) permits both communicating and non-communicating devices to communicate and to engage with each other [5]. The purpose of IoT is to establish an improved surrounding for the whole humanity which will automatically figure out the needs of people and perform accordingly[6]. From the private user's point of view, the most apparent effect of the introduction of IoT will be seen in both working and domestic fields. IoT connects several technologies from different fields together to build its network. The summation of Internet based and context aware services along with these different technologies, provide a dynamic platform for IoT. Since the last 15 years, IoT has acquired major interest from the industry as well as educational field due to the abilities that can be proposed by IoT. IoT assures to develop the world where all the things around us will be linked to the Internet and information will be shared with one another with minimum human interference.

Internet-of-Things (IoT) is mainly a mesh of intelligent equipment including actuators, sensors and inherent chips which gather data about their equipment, ambience and convey it to global network. People and other devices use this data, to get exciting details and attain quicker solution[2]. IoT provides the main benefits of the automating the daily activities and real time supervision of equipment and functions. IoTs has ability to reform all field-of-life. As IoT has its application worldwide, complexity is increasing with the increase in IoT usage. This complexity brings IoT to vulnerability for the cyber-threats. The actual equipment in IoT is located in insecure places which might be unprotected from hackers, therefore providing themselves the chance to modify the data that move through the mesh. Thus, equipment, permissions and data root should be main issues

[8][2]. Furthermore, IoT develops responsive personal information over their proprietors and this information is handled by central companies that bring critical issues about integrity and confidentiality of data.

In recent days, Blockchain has appeared as the innovation that has ability to manage the issues which are experienced by IoT equipment. In the Blockchain inception, it has drawn the attention of scholars from the whole world, as the advantages of Blockchain are far reaching.

In 2008 Satoshi Nakamoto first gives the concept of blockchain when he issued "Bitcoin: A P2P Electronic Cash framework". Suggested framework was established on encrypting proof rather than precision, authorizing any two participants to perform operation without the needs of a reliable middle man[3]. Blockchain has proved a useful tool in many industries, as well as the Internet of Things. Blockchain mechanism mentioned as an open record and all performed operation are registered in a record of blocks[4]. Proof-of-stake / proof-of-work are used to create and maintain blocks. Each block includes the hash address of recent block that preserves the transactional information in network.

This information is permanent and can be watched entire duration of the mesh which finally brings to achieve the interest of human in the mesh[2]. This interest urges the human to build cash transactions, which provides a new globe of economical division in the domain of IoT. To secure the data of user, algorithms implemented in blockchain are named as public key encryption and shared concord algorithms.

The main features of blockchain technology are usually audit ability, persistency, decentralization and anonymity. The large and encouraging field of blockchain mechanism gives higher support in the academia to the learners and institutions. Considering every area of life, the blockchain mechanism is not restricted to over discussed application. The applications are raised in fields such as IoT, business, governance, medical and education etc. Furthermore, the blockchain mechanism eliminates the middle man by spreading of influence apart from the middle man in health, transmission, education, law and politics.

A systematic literature review is conducted in our paper to highlight the issues that occurs in the field of IoT and also described features of blockchain technology that will help to solve these issues. The remaining part of the article is organized as follow. In segment 2, Blockchain and its enclosed properties are examined. Segment 3 provides a summary of our review strategy & motivation behind leading this literature review. Segment 4 is distributed into three parts, Part 1 emphasizes issues in the IoT field; Part 2 analyzes how BC (Blockchain) can be utilized to solve these issues; Part 3 emphasizes issues in IoT that should be resolved. Part 4 discusses Blockchain implementation issues in IoT's. At last, segment 5 covers the conclusion & future Work.

2. FEATURES OF BLOCKCHAIN

A. Decentralization

Decentralization can be reviewed as a security framework against hackers[2]. Blockchain is a de-centralized normal open logbook where all hubs are related with each other in a cross-linked meshwork, where all the information and decisions-making is set and split among different hubs. All parties can see every transaction on Blockchain. It permits to stay away from the congregation of power that could let an individual to take control on entire arrangement. It provides an intermediate free setup[4]. A decentralized Blockchain mechanism helps to tackle the issues of validation of the client, dependability of outsider and reliability of transactions.

B. Immutability

Digital ledger gives a temper proof atmosphere where upon every information has been saved in block, it cannot be modified or eliminated[3]. The immutability idea of Blockchain is the same as the idea of "Heihachi Mishima" in the film named "Tekken"[2]. Both ideas are set up on immortality which implies neither alterable in any manner. In that event there is some instability by exterior hubs, the hash key worth's could be modified that these keys are encrypted connected with both preceding and previous blocks and corrections in records will trespass the constancy of keys. It implies that the Hash-function in Blockchain has capability to save the recent value or address which is self-generated by the framework over entire transaction client gives. Immutability works totally relies upon 51 percent assent having proof of work.

C. Traceability

The traceability Blockchain enables the clients to decide and follow the cause of any transaction with the assistance of a digital signature. Traceability is additional element beyond the achievement of the Blockchain. Each transaction in the blockchain associated with each other which make a chain[2]. By viewing the chain, information can be followed from inbound to outbound. E.g., a client has to distinguish where and how a nourishment thing was made. Traceability will give specific data on that precise nourishment thing producer, its creation, provided crude material information's, shipping request spot, and goal. This suggests clients may follow the state of good as it experiences the periods of the production network[4]. This should be profitable for the client to be delighted with the manufactures and product to view at peaks and valleys in the order.

D. Trustless Network

The idea of a mediator or third party has expelled by the help of blockchain technology, when two participants want to get confirmed and a while later the transaction method will happen[24]. On Blockchain any customer can verify Proof-of-work (POW) of some different element, in this manner client validation from an outsider is not mandatory[25]. This

gives a quicker, dependable and secure method for transactions. Another backbone of Blockchain called "Self-execution" wherein the owner will compose an contract of their items and at one time it fixes any determination buyers, it will be executed though customer input. As the contacting equipment on the Blockchain mesh are quite a semi or completely computerized, a superior opinion can be built in fewer time forestalling the component of human defects.

E. Consensus mechanism

Accord system implies the regular confirmation of the considerable number of hubs identified with the blockchain network[3,26]. In this way, it doesn't rely upon third-party. A couple of strategies for consensus mechanism are Proof-of-work (POW), Proof-of-stake (POS), and delegated proof-of-stake (DPOS).

F. Smart contract

A computerized PC program running on a blockchain share network is known as a smart contract[4]. It is a strategy of dispersal of computerized assets among minimum two participants naturally expressed by the equation decided based on information that is inspected at the period of surrounding up the contract[28]. A smart contract is a PC program that forced its accomplishments on blockchain enrolled by the accord protocol. The consensus expresses that the authentication will be completed if all hubs on network sustain the transaction.

G. Security

The influence or the association of outsider or third party is wiped out in block chain technology as this technology is totally established on P2P network[27]. The consensus mechanism is utilized for transactions and the hashes of previous block and time-stamp is contained in block that is used for the validation of transaction[4]. Transaction, synchronization of transactions with hubs on the network is ceaseless and the historical backdrop of transaction remains noticeable. This P2P and accord based nature of BCT provides the security to data of transactions.

Comparison of secondary studies

Since Blockchain innovation is slightly recent in the area of the science, so a most part of research is in progress. While finding for secondary studies, we have identified two papers that work on systematic literature review [1][2] of IoT and highlighted the main issues of IoT solved with blockchain. On other hand in our research, we have highlighted the security issues of IoT and their solution with blockchain features. Moreover, we have also highlighted some IoT security issues that are needed to be addressed.

3. SEARCH METHODLOGY

This area includes the techniques, methodologies, and reasons to compose an SLR (systematic literature review) paper on the present issues of the IoT field and how to fathom these types of issues utilizing Blockchain mythology. Furthermore, it will offer help for scholars to figure out either the integration of IoT and Blockchain is efficient or not?

A. Motivation and Research Questions

In the present condition, IoT equipments have discovered their path in about entirely each area of human life beginning from institution, small companies and indeed they have entered in depth in the life of ordinary person. In addition to the huge interest provided by these equipment, they additionally have plenty of issues. In our article, we have pointed out some issues relevant to the IoT field and simultaneously gave the solution of these issues by using the blockchain features. In addition, we also pointed out those issues in this article, that occur after utilizing the blockchain in IoT see Table 1

TABLE I. RESEARCH QUESTIONS

Sr. No	Research Question	Motivation
1	What are the issues relating to IoT?	Goal is to highlight the security issues faced by IoT devices
2	Which Blockchain features are used to solve identified issues?	The purpose is to search out features of Blockchain that will assist in settling issues of the IoT.
3	What are the IoT issues that are needed to be resolved?	The goal is to list down those issues that are not addressed by using blockchain
4	What are the Blockchain deployment issues in IoT's?	The goal is to figure out the issues that emerge during the deployment of Blockchain in IoT.

B. Search Strategy

Related to our keyword IoT and Blockchain we browsed research papers in Springer, IEEE, science direct, and ACM and figure out various results. Afterwards, we pointed out some research papers that were similar with our concern and arrange these papers in systematic form. On Google Scholar we furthermore identified various papers by forward and in reverse searching.

C. Insertion& elimination criteria

Furthermore, related to our search keyword we selected 150 unique research papers. We studied these papers. After examination of conclusion & abstract, we eliminated some research papers that were unrelated and we found around 34 research papers that were entirely similar to our concern.

D. Data abstraction

At last, a distant review of the chosen research papers, various issues are expressed through making a figure utilizing the X-mind software of every issue. Figures are also made to describe the issues that have been tackled through the Blockchain.

4. REVIEWING RESULTS

This segment shows the real findings derived from obtained review of composed research papers. We segmented it into four parts. In the 1st Part, issues in the IoT domain are pointed out as well as their concise introduction. In the 2ndpart, the assessment is made on the judgment of these issues using Blockchain. Additionally we also introduced a solution for certain issues that are examined in various relevant essential studies and are not be resolved by utilizing blockchain till now. Part 3rd emphasized issues in IoT that should be resolved. Part 4th Blockchain Implementation issues in IoT's?

A. RQ1: What are the issues regarding to the domain?

a) ***Single point of failure:***Nowadays single point of failure is a big problem while creating IoT devices network for data storing. When a centralized network is established by connecting different IoT devices than security and availability of data is on risk[18]. In this network all device are connected with a centralized party and data is kept by third party at one place and it's very easy for any hacker to access that point. After overcoming the centralized system hacker will able to access the data[29]. This causes unauthorized data manipulation. Another thing is single point of failure which means that if centralized system stops working or crashed due to any reason the whole network will be crashed and cause a lot of issues for all devices as well as for relating users.

b) ***Different Computational Power of IoT Devices:***The rising emission of tiny programmable built-in equipments that are simply linked with network through broadcast technologies had risen the quantity of participants eligible to take part in IoT mesh that can share data. From this point of view, the formation of tiny interconnected equipments is helpful for not just sharing of data additionally give an edge in IoT equipments sharing that can interrupt, in a bad and decent both ways, with the adjacent atmosphere[17]. If we implement this scheme to a geographic field, for example, a city or a state, we can envision a full ambit of the ground made by movable equipments that gather information and send them back to a focal bunch endpoint. The information assortment system works by joining the estimations obtained by the cell phones with the approval procedure made with particular mining software that handles the information. In this mesh mobile equipments can perform a significant role.

If this network's data is stored at a central point, a lot of issues will occur. While creating a network board, different types of hardware are used. This board has a lot of tiny sensors deployed on it that will use a low voltage of energy. As the size will decrease, the computational power and input will be decrease, on the other hand, some of the hardwares will be greater in size automatically consume much energy[30]. Therefore tiny sensors and large hardware consumption power and also computational capability are indirectly proportion to each other. This will cause a problem in calculation of results. On the other hand, portable devices will cause an issue like in movement of any devices in different geographical area so to change the distance and connectivity mechanism of devices one by one will prove hectic for administrator.

c) ***Data Integrity:*** It is the training of being sincere and demonstrating a reliable and inflexible compliance to ethical standards and persistent moral and values in morals. Integrity is considered as the authenticity and honesty or precision of one's actions. In a central client server model, the offender may acquire prohibited access to the mesh and change the first information or original data and forward it[7,8]. For instance, Bob sends information to Watson. Alice the center person may get information first and forward the information after alteration.

d) ***Data Authentication****:* Authentication is essential for building a link between two equipments and the swap of some private and public keys through the hub to avoid information stealing[10,11]. Any escape clause in security at the network layer or huge overhead ensure transmission may reveal the mesh to an enormous number of vulnerabilities.

e) ***Denial of Services:***Attackers may approach to the smart home mesh and send bulk SMS to smart equipments, especially, Request to Send (RTS)/Clear to Send (CTS)[9]. They can furthermore attack to specific equipment by utilizing harsh codes so as to perform DOS attack on different equipments that are linked in a smart home. Subsequently, smart equipmentscan't perform appropriate functionalities through venting resources because of such attacks. For prevention from this attack, it is essential to apply authentication to block and identify unauthorized access.

f) ***Trespass:***In case the smart door lock is accessible by an unauthorized party or it is affected by pernicious codes, the attacker can violate on the smart home without splendid the doorway. The outcome of this impact could be a death toll or property. IoT in smart Home the IoT Smart Home facilities are increasing step by step, digital equipments can efficiently communicate with one another by using Internet Protocol (IP) addresses. In smart home Environment, each smart home equipment is attached to the internet. The possibility of malevolent attacks is increasing by the no of equipments increase in the smart home environment[9]. In Case the smart home equipments worked separately.The odds of pernicious attacks also decrease. At present smart home equipments can be on-access by using the internet at any place whenever. In this way, it rises the odds of pernicious attack on these equipments.

g) ***End-to-End security:***Security at the end-points Internet hosts and IoT equipmentsare similarly significant. Using cryptographic schemas for encryption and verification codes to packets isn't enough for asset obliged IoT. For

complete end to end security, the verification of specific personality on the both ends, protocols for actively negotiate session keys, (for example, IPsec and TLS), and algorithms (for instance Hash and AES algorithms) must be safely implemented[10]. In IoT with end to end security, the both ends can ordinarily depend on the reality that their transmission isn't apparent to any other individual, and nobody else can alter data in carriage. Proper and whole end to end security is needed, without which numerous applications would not be feasible.

h) ***Trusted accountability:***Another attack called history revision attack, is brought up in [34]. The authors express that, for the situation, an attacker possesses a computational intensity numerous of the computational intensity of legit hubs in IoT private network for association (for example, two times higher), it is capable to generate a branch of the blockchain which could pass the current one in conditions of challenges of the POW, thus could be acknowledged by different equipments, therefore modifying the historical of the mesh[1]. At the point when scam miners will conquer the mesh and would attempt to change the past history, this will cause a major issue for the mesh.

i) ***Interoperability and Standardization:***Equipments made by different vendors vary in services and technologies, therefore making them inconsistent[2]. As all the items would be linked through the means of Internet, consequently the task of consistency should be changed to give interoperability among the different objects and sensor hubs inside the remote sensor networks.

B. RQ2: The features of Blockchain used to settle the specified issues.

a) ***Single point of failure:***Blockchain is a decentralized P2P network in which all the connecting hubs can share information[18]. In blockchain network all the nodes sync their storing information and compare it with one another. All the participant hubs in blockchain mesh share the same information and there is no single point for storing. In blockchain all the nodes have the capability to store same type of data, so in blockchain based network, if any irrelevant node (Hacker) wants to access the data by **fake,** it is much difficult task for that node. If that irrelevant node succeeds in accessing the data and wants to make some changes will be able to change the data of only one node for a short time because when data will be updated, all the nodes will sync their information with one another and in case of any vulnerability in data, they will update themselves according to the linked information and the fake user will be terminated from the network. In second scenario if any of the point get crashed, then that node will be connected to the network.This can update their whole data according to all other nodes. So in this way single point of failure in blockchain network will not disturb the whole network.

b) ***Different Computational Power of IoT Devices:***Ethereum platform is to record assessments coming from the IoT mesh of sensors. In our frame of work, sensors are IoT equipments, customized to be associated with the blockchain and ready to send messages.

While using Ethereum platform a smart contract will be defined for all IoT devices according to need. By using smart contract these issues can be resolved[17]. In a city sense, Blockchain author has suggested a wonderful blockchain based solution to sort out this kind of issues. For example smart contract will be defined for low computational power devices according to their supporting power. On other hand smart contract will automatically handle the energy need of all devices while making this network, user will write a code in the form of Smart contract that any change occurred in system according to need, will change the whole network according to requirements. Another thing that is discussed in this issue, is movement of portable devices, smart contract will able to change the location geographically and connectivity of a particular device according to predefined description. Using smart contract methodology all the networks will be settled one time and thenwill update themself automatically according to required scenario.

c) ***Data integrity:***Blockchain is a P2P uniform network wherein all hubs have a similar duplicate of records[8]. At the point when a transaction is started, the initiator hub signs the transaction with its private key and sends it to different hubs for approval. All other excavator hubs participate in repeal process and attempt to discover nonce. The hub which finds the nonce initially has the privilege to approve and get the benefit. In addition, it will communicate to every other hub of the whole network. When the record is stacked in the blockchain it can't be altered Rollback or deleted.

d) ***Data Authentication:***Authentication's Issues can be settled by establishing up a trustless network, that is the key element of blockchain. By scheme, information transmitted by IoT equipments associated with the blockchain network will consistently be cryptographically proofed and marked by the real sender that holds GUID and a special public key, and in this manner securing integrity and authentication of transmitted information. Also, all transactions made by an IoT equipment are noted on the blockchain distributed ledger and can be monitored safely. Before sending them to different equipments the message will be digitally signed by the Sender. The recipient equipments then receive the public key from the record and use it to confirm the computerized signature of the obtained message[12][13]. We have explained the computerized signature work in the following way: 1st, the sender evaluates hash of a message that is then encoded with its private key. The computerized signature as well as the message is transferred. The recipient at that point decodes the computerized signature utilizing the public key of the sender retained in the record to get the hash value as evaluated by the sender. The message is authentic just if the evaluated hash and the protective hash of the message are similar. The trust on acquired messages are enhanced if the computerized signature of every message is saved into the ledger.

e) ***Denial of Services:***In a blockchain network, two stages are significant to verify the network from DOS. The 1st

stage of defense can be assigned to the reality that it would be unfeasible for an attacker to instantly install malware on IoT equipments since these equipments are not directly accessed. Each transaction must be checked by the mining hubs[14].

Let us for an instant expect that the attacker in some way quiet control to infect the equipments. The second stage of defense originates from the fact that all cordial traffic must be approved by the extractors by inspecting the scheme header. The scheme header is utilized for authorizing equipments and imposing the proprietor's control scheme over the network. Since they enquires that establish the DoS attack traffic would not be approved, they would be impeded from withdrawal of the network. The following two defense stages are especially set up and overseen by the target of a DoS attack that can be any client in the overlay.

f) ***Trespass:***Use of Blockchain based smart home network prevents the interference of any middleware[8]. In this network all the included devices have their own storage capacity which contains similar records of all other devices also contain input transaction given by the user. When a new user will try to interfere in network give any input, the related device will verify the input transactions and previous history in blockchain. If the IoT devices find the similar history in previous data it will grant permission to the user otherwise rejected. In other scenario, if the middleware succeeds in controlling the IoT device in smart home network, meanwhile the device will match its details with other device. In case of miss match it will be updated automatically according to the BC smart home history and hacker will be disconnected. Hence the Blockchain innovation makes the equipments competent for performing tasks without the third party or mediator, in this manner making it danger free from mediator.

g) ***End to End Security****:*The session determined b/w two VoLTE UEs are finished by 3GPP IMS standard with no progressions as explained already, which brings outcomes in the protocol. One of the solutions to produce and disperse the session keys is to utilize the Station to Station (STS) key agreement schemas. The primary benefit of this methodology is the utilization of Diffie-Hellman (DH) as a key swap (Perfect-Forward-mystery)[12,15]. The problem of public keys sharing in DH is tackled by saving them into the Blockchain. The VoLTE UE A guest customer brings the community of the VoLTE UE B called from the Ethereum and conversely. The UE A and UE B switch the DH parameters across RTP Control-Protocol (RTCP).

h) ***Trusted accountability:***Each activity history should be transferred to the blockchain network[8,16]. This provides each activity identification and every activity is detectable. At that point, when an irregular manner is distinguished, entity send to source for extra investigation.

i) ***Interoperability and Standardization:***A distributed arrangement of Firmware could be presented by utilizing Blockchain. Furthermore, the inflexible memory of the Blockchain, Firmware morality could be reliable and the accessibility of Firmware meanwhile proposed equipments could be guaranteed[19]. A Blockchain settled reliable Firmware update schemas is suggested to manage with Firmware issues of IoT's. The design of this schema is included of 'Verification' & 'Normal' hubs in a Blockchain settled network. Ordinary hubs are IoT equipments which can moreover demand a Firmware relevant activity or react to different IoT equipments application. Moreover, to these hubs, there is a 'retailer hub' which maintains updated authentication hub with most recent data[2,20]. Once an IoT inquires a Firmware relevant update, in this (BC) Blockchain network, it acquires a feedback from different hubs to decide if it has most recent Firmware or none. On the off chance that an update is essential, at that point Verification hub gives data about the necessary update and position of its binary. On the off chance that Firmware of equipments arejust latest then morality of exiting Firmware could be confirmed over the Blockchain network.

C. RQ 3: what are the security issues of IoT that are needed to be resolved?

a) ***Falsification:***when the equipments are in the smart home, they carry out transmission with the requested host, the attacker might gather the packets by modifying the routing table in the portal. The secure-socket-layer (SSL) technique is implementing and an attacker can avoid the fake certificate. In such a way, the attacker can misconstrue the substance of information or may release the privacy of information. To protect the smart home network from this offense, the SSL technique with appropriate verification mechanism must be applied. It is too essential to block prohibited equipments that may effort to access to smart home network. The IoT is an idea that describes the prospective where the physical things associated with the internet transmission with one another and recognize themselves for different equipments[9]. The IoT framework comprises of smart things, tablets, cell phones, and the intelligent equipments etc. Such frameworks use RFID, QR (Quick Response) codes or remote technology to execute transmission between various equipments. The IoT supports to establish a connection from person to person, person to physical things, and physical things to other physical things. According to a valuation from IDC, there will be above 30 billion internet linked equipments by 2020. This speedy development of internet data demands furthermore useful and secure network.

b) ***Ubiquity, omnipresence****:*The end-user is attracted to IoT[21], gorged by it, there is no plainly out, an approach to quit up utilizing the antiquities (which will not anymore be feasible eventually, because of the producers which will provide them with Internet linked equipments.

c) ***Miniaturization, invisibility****:*PCs, as they are these days, will vanish – the equipments will be tiny and tiny, apparent, subsequently keeping away from any assessments, accounting procedures, audit and quality control[21].

d) ***Difficult identification****:*So as to be linked with the IoT, the objects are identification[31]. The accessibility to these "armies" of objects, the administration of these

identities may raise huge concern and cause difficult issues of security and control in a globalism.

e) ***Autonomous and unpredictable behavior****:* The interrelated objects may interrupt voluntarily in individual events, in surprising ways for the clients or the developer. The individuals will be a part of the IoT environments combined with equipments and artifacts, therefore making hybrid frameworks with surprising manner[21]. The gradual improvement of IoT will cause of rising manners without the clients completely understanding the environment they are vulnerable.

f) ***Incorporated intelligence***: This produces the objects to be viewed alternative for the public activity – the objects will be dynamic and intelligent, with a rising manner; there will be enlargements (not just outside) of the human body and mind[32]. Being denied of these equipments will prompt issues – see the youngsters who regard themselves as psychologically or socially disabled without Google, social media or cell phone.

g) ***Mobile Security:***Smart phones hubs in IoT repeatedly move from one bunch to another, in which encryption-based protocols are utilized to enable quick recognition, confirmation, and security refuge. A specific protocol is shown which is helpful when a smart phone hub joins another bunch. This protocol furthermore received a legitimate demands message and an answer verification message, which quickly implements authentication, privacy protection and identification. It will be valuable to defend opposing replay attacks, bugging, and location privacy attacks. Conversely with other same protocols[22], for example, essential hash protocols, it has less transmission above, progressively secure and gives more privacy protection. Condensing, additionally if the security issues of cell phones (i.e., equipments authentication and identification, key and exchange and legitimating storage) are under inquiry by scientific society, the accessible arrangements moderately address these requirements, in this way requiring additional attempts in order to enable the coordination with the other IoT technologies.

h) ***Robustness in Connectivity:***In IoT, interconnect the humans and objects through sensors and guaranteeing ensured connectivity is a massive challenge[23]. Furthermore, volatile internet availability represents a significant challenge to the IoT. Henceforth, there is a squeezing need to effort on energy amassing equipments to improve the availability with the assistance of the energy mechanism.

i) ***Big Data:***While big data is relevant from the IoT point of view, we have to guarantee that only appropriate information is being derived from the immense databases[33]. The Information Technology industry is looking ahead to governing the ability of big data and the IoT can highly contribute to collecting more data that would demonstrate useful to the businesses.

D. RQ 4: what are the Blockchain Implementation Problems in internet of things?

a) ***Energy Consumption:***Energy consumption is different in different traffic flows[14]. With the passage of time data increases, when Proof-of-Work is applied on data it takes a lot of time for searching data and also consume more energy. The miner for managing transactions is referred to energy consumption. In the smart home, miner is the most energy-consuming equipment. It performs lots of encryption and hashing and handles all other transactions. The EC (Energy Consumption) of different types of equipments is constrained to cryptography for their own transaction.

b) ***Scalability:***A large quantity of information is produced by IoT's and it will be complicated and costly for the Blockchain to keep up and save this large amount of information. Such inability is primarily because of IoT equipments have restricted substance and there are requirements for similar stationing design where the main segment of information necessary for IoT transactions is kept by IoT equipments[1]. The 2nd Scalability issue is low output, because of the quandary of Proof-of-Work (PoW). Again for restricted ability, IoT's, high challenge of Proof-of-work (PoW) is hard to compute. Bringing down the challenge of Proof-of-Work will make security problems[2]. Actually, this issue is the interchange between security and the scalability. These scalability problems of the Blockchain should be tended in further study as these fabricate the Blockchain badly reasonable for IoTs.

c) ***Anonymity:***The blockchain becomes an open network and the Anonymity is imperative to protect the secret of clients[2]. Tragically, the blockchain just gives alias implies even though clients do not have actual-life identification. The client has a Public key that is utilized to execute transaction on this Open network. By Using this Public ID a client could be tracked. Furthermore, when a client utilizes various Public keys it could be tracked by linked capabilities that these numerous addresses belonging with a similar client. Solution and analysis for the Anonymity of the clients are essential to be tended to in further work.

d) ***Irreversible:***Certainly, the blockchain has amazing properties like a shared block[4], for example, transparency, efficiency, and irreversibility. Although, there are a few drawbacks related to this characteristic of blockchain. Right now, if information is entered inaccurately, at that point it can't alter/delete, because blockchain is a P2P network have not erasable or reversible. In this way, it is a vital issue of blockchain innovation. While the present compromise frameworks permit the way toward reconciliation and voiding, envision the issues of "rollback" in the world of shackles.

e) ***Approval first Network Node****:* Initially, some organization should be first network hub and that moment there will be no available hub to ensure it, security hazard can be viewed as a feature[3]. In any case, we believe that with the enhance in numbers of hubs, such as security issues will be reduced.

5. Conclusion and Future Work

We have described the systematic literature review (SLR) on Blockchain, Internet of Things and pointed out some issues relevant with an IoT field and also introduced the appropriate solutions for these Issues with the help of Blockchain features. Such issues are mostly Data Integrity, Data Authentication, Denial of Services, Different computational Power of IoT Devices, Trespass and security related. Blockchain can support in maintaining security, privacy and supply of non-seller reliant Firmware be updated. Besides, inviolable history of records, Identity of equipments, Integrity of IoT information and access administrating to IoT equipments can be well controlled using the improvement of Blockchain. In addition to the advantages, we further considered some unaddressed execution issues like Anonymity, Irreversible, Scalability, Energy Consumption and Approval first Network Node of Blockchain in IoT's which give further guidance for analysts who are relevant in this field. Considering the writing, Blockchain is an engaging replacement to deal with normal issues being addressed by IoT. Maintaining the ability synergies in see the blend of the two advances is required to alter each field of life.

References

[1] Conoscenti, Marco, Antonio Vetro, and Juan Carlos De Martin. "Blockchain for the Internet of Things: A systematic literature review." In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1-6. IEEE, 2016.

[2] Shehzad, Kamran, Muhammad Afrasayab, Murad Khan, Muhammad Azhar Mushtaq, Rana Laique Ahmed, and M. Mohsin Saleemi. "Use of Blockchain in Internet of things: A Systematic Literature Review." In 2019 Cybersecurity and Cyberforensics Conference (CCC), pp. 165-171. IEEE, 2019.

[3] Yumna, Hafiza, Muhammad Murad Khan, Maria Ikram, and Sabahat Ilyas. "Use of Blockchain in Education: A Systematic Literature Review." In Asian Conference on Intelligent Information and Database Systems, pp. 191-202. Springer, Cham, 2019.

[4] Razzaq, Asad, Muhammad Murad Khan, Ramzan Talib, Arslan Dawood Butt, Noman Hanif, Sultan Afzal, and Muhammad Razeen Raouf. "Use of Blockchain in Governance: A Systematic."

[5] Yogitha, K., and V. Alamelumangai. "Recent Trends and Issues In IOT." International Journal of Advances in Engineering Research (IJAER) 11, no. I (2016).

[6] Dhumane, Amol, Rajesh Prasad, and Jayashree Prasad. "Routing issues in internet of things: a survey." In Proceedings of the international multiconference of engineers and computer scientists, vol. 1, pp. 16-18. 2016.

[7] Ravindran, Rinju, JerrinYomas, and E. Jubin Sebastian. "IOT: A review on security issues and measures." International Journal of Engineering Science and Technology 5, no. 6 (2015): 348-351.

[8] Sultan, Abid, Muhammad Sheraz Arshad Malik, and Azhar Mushtaq. "Internet of Things Security Issues and their Solutions with Blockchain Technology Characteristics: A Systematic Literature Review." Am J Compt Sci Inform Technol 6, no. 3 (2018): 27.

[9] Razzaq, Mirza Abdur, Sajid Habib Gill, Muhammad Ali Qureshi, and Saleem Ullah. "Security issues in the Internet of Things (IOT): a comprehensive study." International Journal of Advanced Computer Science and Applications (IJACSA) 8, no. 6 (2017): 383-388.

[10] Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." In 2014 international conference on privacy and security in mobile systems (PRISMS), pp. 1-8. IEEE, 2014.

[11] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," Journal of Cyber Security and Mobility, vol. 1, no. 4, pp. 309–348, 2013.

[12] Khan, Minhaj Ahmad, and Khaled Salah. "IOT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.

[13] Singh, Madhusudan, Abhiraj Singh, and Shiho Kim. "Blockchain: A game changer for securing IOT data." In 2018 IEEE 4th World Forum on Internet of Things (WF-IOT), pp. 51-55. IEEE, 2018.

[14] Dorri, Ali, Salil S. Kanhere, Raja Jurdak, and Praveen 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), pp. 618-623. IEEE, 2017.

[15] Kfoury, Elie F., and David J. Khoury. "Secure end-to-end volte based on ethereum blockchain." In 2018 41st International Conference on Telecommunications and Signal Processing (TSP), pp. 1-5. IEEE, 2018.

[16] Liang, Xueping, Juan Zhao, Sachin Shetty, and Danyi Li. "Towards data assurance and resilience in IOT using blockchain." In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), pp. 261-266. IEEE, 2017.

[17] Ibba, Simona, Andrea Pinna, Matteo Seu, and Filippo Eros Pani. "CitySense: blockchain-oriented smart cities." In Proceedings of the XP2017 Scientific Workshops, pp. 1-5. 2017.

[18] Durand, Arnaud, Pascal Gremaud, and Jacques Pasquier. "Decentralized web of trust and authentication for the internet of things." In Proceedings of the Seventh International Conference on the Internet of Things, pp. 1-2. 2017.

[19] Lee, Boohyung, and Jong-Hyouk Lee. "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment." The Journal of Supercomputing 73, no. 3 (2017): 1152-1167.

[20] Boudguiga, Aymen, Nabil Bouzerna, Louis Granboulan, Alexis Olivereau, Flavien Quesnel, Anthony Roger, and Renaud Sirdey. "Towards better availability and accountability for IOT updates by means of a blockchain." In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 50-58. IEEE, 2017.

[21] Popescul, Daniela, and Mircea Georgescu. "Internet of Things–some ethical issues." The USV Annals of Economics and Public Administration 13, no. 2 (18) (2014): 208-214.

[22] Balte, Ashvini, AsmitaKashid, and Balaji Patil. "Security issues in Internet of things (IOT): A survey." International Journal of Advanced Research in Computer Science and Software Engineering 5, no. 4 (2015).

[23] Matharu, Gurpreet Singh, Priyanka Upadhyay, and Lalita Chaudhary. "The internet of things: Challenges & security issues." In 2014 International Conference on Emerging Technologies (ICET), pp. 54-59. IEEE, 2014.

[24] K. Christidis and M. DevetsikIOTis, "Blockchains and SmartContracts for the Internet of Things," IEEE Access, vol. 4, pp.2292–2303, (2016).

[25]J. Sun, J. Yan, and K. Z. K. Zhang, "Blockchain-based sharing services: What Blockchain technology can contribute to smartcities," Financ. Innov., vol. 2, no. 1, p. 26, (2016).

[26]Grech, Alexander, and Anthony F. Camilleri. "Blockchain in education." (2017).

[27] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In 2015 IEEE Security and Privacy Workshops, pp. 180-184. IEEE, 2015.

[28]Ojo, Adegboyega, and Samuel Adebayo. "Blockchain as a next generation government information infrastructure: a review of initiatives in D5 countries." In *Government 3.0–Next Generation Government Technology Infrastructure and Services*, pp. 283-298. Springer, Cham, 2017.

[29] Silva, Maria B., Peter S. Nielsen, Niels Bay, and P. A. F. Martins. "Failure mechanisms in single-point incremental forming of metals." The International Journal of Advanced Manufacturing Technology 56, no. 9-12 (2011): 893-903.
[30]Samie, Farzad, Vasileios Tsoutsouras, Lars Bauer, Sotirios Xydis, DimitriosSoudris, and Jörg Henkel. "Computation offloading and resource allocation for low-power IOT edge devices." In 2016 IEEE 3rd World Forum on Internet of Things (WF-IOT), pp. 7-12. IEEE, 2016.
[31] Yu, Dan, Lilong Zhang, Yongle Chen, Yao Ma, and Junjie Chen. "Large-Scale IOT Devices Firmware Identification Based on Weak Password." *IEEE Access* 8 (2020): 7981-7992.
[32] Alonso, Ricardo S., Inés Sittón-Candanedo, Óscar García, Javier Prieto, and Sara Rodríguez-González. "An intelligent Edge-IOT platform for monitoring livestock and crops in a dairy farming scenario." *Ad Hoc Networks* 98 (2020): 102047.
[33] Amanullah, Mohamed Ahzam, Riyaz Ahamed Ariyaluran Habeeb, FarizaHanumNasaruddin, Abdullah Gani, Ejaz Ahmed, Abdul Salam Mohamed Nainar, Nazihah Md Akim, and Muhammad Imran. "Deep learning and big data technologies for IOT security." Computer Communications (2020).
[34]Barber, Simon, Xavier Boyen, Elaine Shi, and ErsinUzun. "Bitter to better—how to make bitcoin a better currency." In International conference on financial cryptography and data security, pp. 399-414. Springer, Berlin, Heidelberg, 2012.

Authors.

First Author Shoaib ul Hassan got his B.S. degree from Department of Computer Science and Information Technology in University of Sargodha, Sub Campus Bhakkar in Pakistan in 2018 and doing his MS degree from Department of Electronic Information and Artificial Intelligence in Shaanxi University of Science and Technology in China. His research interest is focused on Internet of Things, Android Operating System, Blockchain and Cloud Computing.
Email: shoaibbsit14@gmail.com, ls190312@sust.edu.cn

Second Author Jingxia Chen got the B.S. and M.S. degrees from Department of electrical and information engineering in Shaanxi University of Science and Technology in China in 2002 and 2005, respectively. During 2013-now, studied for Ph.D. degree in School of Computer Science and Engineering, Northwestern Polytechnical University in China. Now she also works as an associate professor in Department of Electronic Information and Artificial Intelligence, Shaanxi University of Science and Technology in China. Her research interest is focus on Machine learning and pattern recognition, EEG signal processing and event detection, and deep learning.
Email: chenjx_sust@foxmail.com

Third Author Muhammad Afrasayab got his B.S. degree from Department of Computer Science and Information Technology in University of Sargodha, Sub Campus Bhakkar in Pakistan in 2016 and got his MS degree from Department of Computer Science in Govt College University Faisalabad. His research interest is focused on Internet of Things, Blockchain and Cloud Computing.
Email: afrasayabuos@gmail.com

Fourth Author Ali Akbar got his B.S. degree from Department of Computer Science and Information Technology in Iqra University in Pakistan in 2016 and doing his MS degree from Department of Electronic Information and Artificial Intelligence in Shaanxi University of Science and Technology in China. His research interest is focused on Internet of Things, Android Operating System and Cloud Computing.
Email: aa81079@gmail.com

Fifth Author Muhammad Ahsan got his B.S. degree in Electrical Engineering from University of Lahore Pakistan in 2015 and doing his MS degree from Department of Electronic Information and Artificial Intelligence in Shaanxi University of Science and Technology in China. His research interest is focused on Internet of Things and Artificial Intelligence.
Email:Engr.ahsanbaba@gmail.com

Sixth Author Tariq Mahmood got his B.S degree from Department of Computer Science and Information Technology in University of Sargodha, Sub Campus Bhakkar in Pakistan in 2018 and doing his MS degree from Department of Computer Science in Qurtuba University of Science and Technology in Pakistan. He works as a Visiting Lecturer in Department of Computer Science and Information Technology, University of Sargodha, Sub Campus Bhakkar in Pakistan. His research interest is focused on Internet of Things, Android Operating System and Cloud Computing.
Email: tariqmahmood@yandex.com

TABLEII. ISSUES VS FEATURES

Issues	**Blockchain features**						
	Decentralized/ P2P	Immutability	Traceability	Trustless Network	Consensus Mechanism	Smart Contract	Security
Single Point of Failure	[18]		[2][4]				
Different Computational Power of IoT Devices						[3][4]	
Data Integrity	[8]	[2]					
Data Authentication	[12]			[13][24][25]			
Denial Of Services	[14]				[3]		
Trespass						[8][14]	
End-to-End Security			[4][12]				[15][27]
Trusted Accountability			[3][8]				
Interoperability &Standardization	[2]	[3][19]					