IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 6, 2020, accepted July 24, 2020, date of publication August 5, 2020, date of current version August 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3013946

Survival Study on Blockchain Based 6G-Enabled Mobile Edge Computation for IoT Automation

RAMESH SEKARAN[1], RIZWAN PATAN[2], ARUNPRASATH RAVEENDRAN[3], (Member, IEEE), FADI AL-TURJMAN[4], (Member, IEEE), MANIKANDAN RAMACHANDRAN[5], AND LEONARDO MOSTARDA[6], (Member, IEEE)

[1]Department of Information Technology, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada 520007, India
[2]Department of Computer Science and Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada 520007, India
[3]Department of Electronics and Communication Engineering, Siddhartha Institute of Technology and Sciences, Hyderabad 501301, India
[4]Research Center for AI and IoT, Artificial Intelligence Engineering Department, Near East University, 99138 Nicosia, Turkey
[5]Department of Computing, SASTRA University, Thanjavur 612001, India
[6]Computer Science Division, University of Camerino, 62032 Camerino, Italy

Corresponding author: Rizwan Patan (prizwan5@gmail.com)

ABSTRACT Internet of Things (IoT) and Mobile Edge Computing (MEC) technology acts as a significant part of daily lives to facilitate control and monitoring of objects to revolutionize the ways that human interacts with physical world. IoT system includes large volume of data with network connectivity, power, and storage resources to transform data into meaningful information. Blockchain has decentralized nature to provide useful mechanism for addressing IoT challenges. Blockchain is distributed ledger with fundamental attributes, namely recorded, transparent, and decentralized. Blockchain formed participants in distributed ledger to record the transactions and communicate with other through trustless method. Security is considered as the most valuable features of Blockchain. IoT and Blockchain are emerging ideas for creating the applications to share the intrinsic features. Several existing works has been developed for the integration of blockchain with IoT. But, Blockchain protocols in the state-of-the-art works with IoT failed to consider the computational loads, delays, and bandwidth overhead which lead to new set of problems. The review estimates main challenges in integration of Blockchain and IoT technologies to attain high-level solutions by addressing the shortcomings and limitations of IoT and Blockchain technologies.

INDEX TERMS The Internet of Things, security, blockchain, transactions, transparent, and decentralized, bandwidth overhead.

I. INTRODUCTION

Blockchain is used to generate the large-scale index as security measure for all network communication. It operated as mutual, collective and common ledger. With development of crypto currencies, blockchain technology is said to be disruptive technology. It performed the transition from client-server to secured network. Blockchain is an immutable ledger for performing financial transactions. It has chain of time-stamped blocks associated with cryptographic hashes. It enabled the users in allocating the P2P network in which non-trusting members swap the data without intermediary. Trust is an essential block chain achieved through resultant hash of preceding block for generating the subsequent block. The resulting hash is authenticated by the miner nodes for finding the hash for the subsequent block. A bunch of transactions are coupled into the blocks by using Merkle tree. Merkle root hash is included in the block.

A blockchain is a ledger spreading over the blockchain system. Blockchain comprised many connected blocks. The first block is termed as genesis block without parent block. A block structure comprised:

- Block version - collection of block validation which regulates to proceed.
- Hash of parent block - a 256-bit field that contains a hash value which points to the earlier block.
- Timestamp recording present time in seconds.
- Nonce from 0 and improve hash computation.
- Number of transactions
- MerkleRoot – accumulates hash value of all the transactions in the block.

The associate editor coordinating the review of this manuscript and approving it for publication was Rongbo Zhu.

A blockchain is developing with the executed transactions. Once block is produced, all nodes are included in block corroboration. A validated block is included at the ending of blockchain by the reference symbolizing the parent block. The emerging technology has large potential impacts in many technological areas and Internet of Things in various aspects with decentralization, communications, transaction models and independent device coordination as described in [1]. The objective was to provide the ideas with structure and operation of Blockchain to examine technology usage for improving the privacy level in IoT. But the computational cost was not minimized. A new framework with layers termed Blockchain Structures (BCS) was introduced in [2] to identify association between IoT and BC for verification. Every BCS was arranged through Blockchain technology. However, it fails in improving the security level.

The Blockchain and IoT technologies was integrated in [3] with high-level solutions for handling the shortcomings and limitations of both IoT and Blockchain technologies. Identification of exact problem in IoT and Blockchain technologies was not performed. The comprehensive review was carried out in [4] with block chain and IoT integration. The objective was to examine research trends on BC-related technologies in IoT context. It studied different application domains and arranging the literature with categorization but failed in resolving the complexity issues.

The centralized architecture was constructed in [5] for minimizing the computational overhead. A distributed access control method was developed for device-to-device communication in IoT-enabled computerization. The security and privacy preservation were essential problems in centralized architecture. But, energy consumption of centralized architecture was higher. Channel State Information (CSI)-free strategies were introduced in [6] with large number of devices. CSI reduced as powered devices count gets increased. The distributed CSI-free plans increased energy coverage region with high reliability. However, the execution time was found to be higher.

A comprehensive review of machine learning was carried out to identify potential benefits and problems for applications in 5G networks. QC-assisted and QML-based framework was introduced in [7] for 6G communication networks through addressing challenges. But it failed in improving the reliability level. Optical wireless communication (OWC) served 5GB communication system demands. OWC technologies were used in [8] for exploitation of 5G/6G and IoT. The communication overhead of OWC served 5GB communication system was higher.

The key technologies were reviewed in [9] to recognize every feature. Teraherz (THz) communications were employed to maintain mobile ultra-broadband, symbiotic radio and satellite-assisted communications. However, data integrity was lower. An integrated IoT platform with blockchain was introduced in [10] to assure the sensing data integrity. The main aim was to pay for device owner for effortless access to the devices in diverse areas. It presented the features of IoT systems for monitoring and controlling the end user. But communication overhead remains unaddressed. A secure and intelligent architecture was constructed in [11] for wireless networks through joining AI and blockchain to allow secure resource sharing. A blockchain empowered content caching issues were addressed to increase the system effectiveness and establish caching scheme through deep reinforcement learning. In secure and intelligent architecture, the privacy level of data was poor.

The security module of IoT device was introduced in [12] depending on blockchain technology to avoid hacking and information infringement. The designed technology formed blockchain system with multi-security among IoT and user device. However, security level was not enhanced through authentication. The new technologies were introduced in [13] with wireless networks towards 6G for several cases. A full-stack, system-level viewpoint on 6G requirements were reviewed and chosen 6G machineries through introducing new communication models. But, central authority was not provided for enhancing the security level. A decentralized and cryptographically strong platform was introduced in [14] with immutability to avoid central authority utilization for authentication and communication. However, data confidentiality level was not improved. The blockchain technology addressed the problems with new facilities like distributed to improve the security level. Distributed ledger technologies were introduced in [15] to present solution for security and privacy problems. Though privacy was preserved, the execution time was not reduced. Table 1 describes the list of abbreviations in the article.

TABLE 1. List of abbreviations.

Acronym	Explanation
IoT	Internet of Things
BCS	Blockchain Structures
CSI	Channel State Information
OWC	Optical wireless communication
5G/6G	5 Generation/6 Generation
THz	Teraherz
BC	Blockchain
BCoT	Blockchain of Things
mMTC	massive Machine Type Communications
D2D	Device-to-Device
DDoS	Distributed Denial of Service
SCM	Supply Chain Management
IoV	Internet of vehicles
DLTs	Distributed Ledger Technologies
CDNs	Content Delivery Networks

A. RELATED WORKS

Several review papers distributed by various authors on blockchain in 6G-enabled IoT for automation.

Scope of Survey: As per the requirement of the survey paper, research in the direction of IoT and BC is to be considered. A lot of research is required to be done for addressing the issues of security with the blockchain technology solution. Research is to be carried out to enable the scalability of the integrating blockchain with IoT. Many reviews based on author knowledge concentrated on security problems and determined the suitability of block chain to perform secured communication. A study was also taken for block chain technology, 6G network, IoT with taxonomy of the security problems. However, a complete survey that focuses all probable security susceptibilities of communication system is not available. Some literatures failed to portray about the incorporation of block chain technology and 5G network. In [16], the effectiveness of combining blockchain for IoT in different applications was presented by studying Blockchain-enabled Intelligent IoT framework with Artificial Intelligence. But computational power and latency issues were not resolved.

Later, Blockchain based decentralized application was employed in [17] for allowing IoT edge processing. It remains possible for the resource owner to integrate the ecosystem and provide necessitated resources. Edge computation was carried out by IoT devices to resource owner nodes if needed. An architectural framework was studied in [18] to enable blockchain in IoT applications. An oneM2M-based IoT platform and blockchain system termed Logchain was employed to guarantee block integrity. But security issues remains unaddressed. Blockchain and Edge Computing were joined in [19] to deal with the inhibited nature of IoT. Framework was constructed to minimize IoT device needs for memory capacity and to enhance performance results. The challenges were evaluated with the Blockchain and Edge Computing architecture. However, resource optimization was not performed. The techno-economic factors and normative assumptions were taken in [20] to enable the propertization. Blockchain applications include the results opposite to intended ones for contributing the IoT based user privacy. But, the privacy level of data remains low. In [21], the convergence of blockchain and IoT was discussed. However, the data analytics on blockchain data remains difficult. A full-fledged approach for the engineering was developed in [22] by combining the Aggregate Computing and Opportunistic IoT Service models. But the computational complexity remains unaddressed. The opportunities and challenges associated to blockchain convention in 6G were discussed in [15]. However, Security level was not enhanced. The reshaping and conversion of DTs by Blockchain was discussed in [23] to secure manufacturing. But privacy issues were not concerned. In [24], the utilization of blockchain for value extraction in 5G was discussed. The existing centralized architecture was described in [25] for handling the huge volume of data created in the IoT. It experiences security and privacy issues. The key characteristics of cognitive-inspired computing were explained in [26] for resolving the security and privacy issues. An intelligent data fusion algorithm based on hybrid delay-aware clustering (HDC) was presented in [27]. The clustering patterns of the cluster were chosen by the decision function to achieve optimize between network delay and energy consumption. However, the execution time was higher.

Dynamic spectrum access algorithm was designed in [28] depended on game theory to perform spectrum leasing and interference mitigation among Secondary Users. But computational cost remains higher. In order to resolve the security issues, counter the threats and to provide efficiency, a new authentication scheme for demand response management was designed in [29]. But the data integrity level remains lower.

Later, A temporal credential based anonymous lightweight authentication scheme (TCALAS) was developed in [30] for Internet of Drones (IoD) networks. TCALAS provided security against threats. In [31], a secure routing and monitoring protocol with multi-variant tuples using Two-Fish (TF) symmetric key approach was designed. It helped to avoid the adversaries in the global sensor network. But the reliability level was poor. Table 2 explained the summary of surveys and variations with proposed review.

B. CONTRIBUTION OF THIS SURVEY

At present several review papers were examined in literature, however the possible security problems of blockchain enabled IoT with 6G were not addressed anywhere. The main contributions of the article are:

- Examine the security problems with blockchain enabled IoT with 6G communication network and describe comprehensive analysis on it.
- Establish an in-depth study of research challenges in incorporation of blockchain with 6G communication network.
- Address the open problems and suggest the future research guidelines toward blockchain enabled IoT with 6G communication.

C. ORGANIZATION AND READING MAP

The organization of this article is illustrated in Figure 1: The outline of blockchain technologies with blockchain benefits for 6G is explained in Section 2. In Section 3, integration of IoT in blockchain is discussed. Section 4 describes the research challenges of blockchain with IoT enabled devices. Section 5 portrays blockchain and IoT integration solutions. Section 6 explains the application of blockchain with 6G enabled IoT devices. Section 7 concludes the paper.

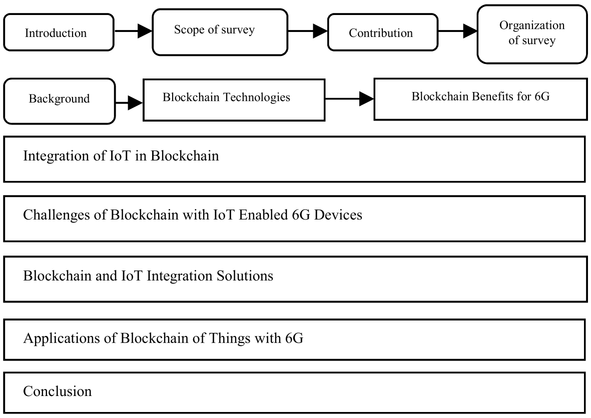
Introduction
Scope of survey
Contribution
Organization of survey
Background
Blockchain Technologies
Blockchain Benefits for 6G
Integration of IoT in Blockchain
Challenges of Blockchain with IoT Enabled 6G Devices
Blockchain and IoT Integration Solutions
Applications of Blockchain of Things with 6G
Conclusion

FIGURE 1. Structure of survey article.

TABLE 2. Challenges of blockchain with IoT for 6G.

Author Name	Technique Name	Contribution	Blockchain	IoT	5G/6G	Vision/ Challenges	Application	Limitations
Emanuel Ferreira Jesus et al. [1]	Transaction models	It provides ideas with structure and operation of Blockchain to examine technology usage for improving privacy level in IoT	Yes	Yes	No	No	Yes	Computational cost was not reduced
Chao Qu et al. [2]	Blockchain Structures (BCS)	BCS identify the association between IoT and BC for verification	Yes	Yes	No	No	Yes	Security level was not improved
Mohammad Maroufi et al. [3]	Blockchain and IoT technologies	The technology provided high-level solutions for handling shortcomings and limitations	Yes	Yes	No	Yes	No	The exact problem was not identified with designed technologies
Alfonso Panarello et al. [4]	Block chain and IoT integration	It examined research trends on BC-related technologies in IoT context	Yes	Yes	No	Yes	No	Complexity level was not minimized
Ishan Mistry et al. [5]	Centralized architecture	The centralized architecture reduced the computational overhead	Yes	Yes	Yes	Yes	No	Though the computation overhead was reduced, the energy consumption remained unsolved
Onel L. AlcarazLópez et al. [6]	Channel State Information (CSI)-free strategies	CSI reduced as powered devices count gets increased. CSI-free plans increased the energy coverage region with high reliability.	No	Yes	Yes	No	Yes	Execution time consumption was not reduced
Syed Junaid Nawaz et al. [7]	QC-assisted and QML-based framework	It identified potential benefits and problems for applications in 5G networks	No	No	Yes	Yes	Yes	Reliability level was not improved.
Mostafa Zaman Chowdhury et al. [8]	OWC technology	Optical wireless communication (OWC) served 5GB communication system demands for exploitation of 5G/6G and IoT	No	No	Yes	Yes	No	Communication overhead was not minimized by OWC technology
Lin Zhang et al. [9]	Teraherz communication technology	Teraherz (THz) communications maintained mobile ultra-broadband, symbiotic radio and satellite-assisted communications	No	Yes	Yes	Yes	No	Data integrity was not improved
Lei Hang et al. [10]	Integrated IoT platform with blockchain	Integrated IoT platform with blockchain assured sensing data integrity. The main objective was to pay for device owner to devices in diverse areas	Yes	Yes	No	Yes	No	Communication overhead was not reduced
Yueyue Dai et al. [11]	Secure and intelligent architecture	Secure and intelligent architecture increased the system effectiveness and establish caching scheme through deep reinforcement learning	Yes	No	Yes	Yes	No	Privacy level was not improved
Bong-Gyeol Choi et al. [12]	Security module of IoT device	Blockchain technology was used to restrict hacking and information infringement	Yes	Yes	No	Yes	Yes	Authentication was not carried out to improve the security level
Marco Giordani et al. [13]	Full-stack and system-level viewpoint technology	A full-stack, system-level viewpoint on 6G requirements were chosen 6G technologies through communication models	No	No	Yes	Yes	Yes	No central authority exists for security enhancement
Asutosh Kumar Biswal et al. [14]	Decentralized and cryptographically strong platform	Decentralized and cryptographically strong platform with immutability avoid central authority utilization for authentication and communication	Yes	Yes	No	No	Yes	Data confidentiality level was not improved

TABLE 2. ***(Continued.)*** **Challenges of blockchain with IoT for 6G.**

Ngoc Tran et al. [15]	Distributed ledger technologies	The designed technology present solution for security and privacy problems	Yes	No	Yes	Yes	No	Privacy preserving time was not minimized
Pankaj Mendki [17]	Blockchain based decentralized application	The designed application assisted resource owner to integrate the ecosystem and provided optimum resources Edge computation was carried out to resource owner nodes	Yes	Yes	No	Yes	Yes	Execution time was higher
ChangHyung Lee et al. [18]	Architectural framework for blockchain in IoT applications	Logchain was employed to guarantee block integrity	Yes	Yes	No	Yes	Yes	Security issues remains unaddressed
Amalia Damianou et al. [19]	Blockchain and Edge Computing	Deals with the inhibited nature of IoT to minimize for memory capacity and enhanced performance results	Yes	Yes	No	Yes	No	resource optimization was not performed
Roberto Casadei et al. [22]	Full-fledged approach	The designed approach combines both Aggregate Computing and Opportunistic IoT Service models for engineering of complex "Edge of Things" applications	Yes	No	No	Yes	No	But, the computational complexity remains unaddressed
Ibrar Yaqoob et al. [23]	Blockchain technology	Blockchain technology refines the concept of DTs for secure manufacturing	Yes	Yes	Yes	Yes	Yes	Privacy issues were not concerned

II. BACKGROUND

The background and history of blockchain, 6G and IoT is explained in this section. In addition, how IoT affects the 6G communication and how BC secure communication networks are described.

A. BLOCKCHAIN TECHNOLOGIES

A sequence of blocks linked by hash value of preceding block is termed as Blockchain (BC). A block accumulated the data. In BC, authority gets decentralized where each member of BC network legalizes the transaction. Every transaction gets marked and validation is carried out through verifying the transaction by the entire mining node in network. The node included immutable transaction records between BC parties. BC addressed the third-party system requirements for performing efficient transaction. It lessens the processing time and cost in performing the transaction over the blockchain network. When miner node transmits new block to decentralized BC network, each member of BC consists of a choice to include block.

Blockchain enhanced the interoperability, privacy, security and scalability during the data communication. A blockchain was combined with IoT and named as Blockchain of Things (BCoT). BCoT comprised of the following merits:

The capability of communication with physical system and information exchange among the IoT systems is defined as Interoperability. Blockchain-composite layer constructed on P2P network with standard access among various IoT systems.

Traceability of IoT data is potential of detecting and authenticating the spatial and temporal data of data block. In blockchain, each data block comprises historic timestamp.

The data quality being trustworthy is defined as reliability of IoT data. It is guaranteed through integrity by cryptographic mechanism with asymmetric encryption methods, hash functions and digital signature. Autonomic interaction of IoT system characterized the potential of IoT system cooperating with each other without third party. The autonomy is attained through smart contracts allowed through the blockchains. The contract clauses in smart contracts get implemented when condition is satisfied. Blockchain is not same as distributed systems depending on the consensus property.

Trust-less: The network entities are indefinite to other. They converse, assist and team up with others devoid of deliberating them. No specialized digital identity is necessitated to carry out transaction between entities.

Permission-less: Restriction is not provided for functioning within the network.

Censorship resistant: Any persons interact with others on blockchain. The confirmed transaction is not modified. Blockchain technology included four components:

Consensus: Proof-of-Work protocol verifies every action in network for avoiding single miner node from managing blockchain network and for manipulating the transaction history.

Ledger: It is shared and distributed database with information about all transactions performed within the network. It is undeniable through nature where information once stored is not deleted. It guarantees that every transaction is verified and accepted as valid one though many clients at particular time.

Cryptography: It guaranteed that all network data is secured with the strong cryptographic encryption. It allowed the authorized users to decrypt existing information.

Smart Contract: It is employed to validate and verify the network participants. Blockchain are categorized depending on managed data, availability and access control.

Figure 2 describes the architecture diagram of blockchain in 6G. Every challenge is clearly described below.

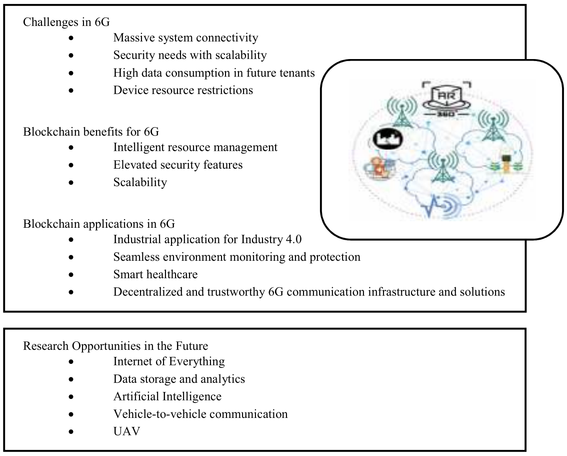
Challenges in 6G
• Massive system connectivity
• Security needs with scalability
• High data consumption in future tenants
• Device resource restrictions
Blockchain benefits for 6G
• Intelligent resource management
• Elevated security features
• Scalability
Blockchain applications in 6G
• Industrial application for Industry 4.0
• Seamless environment monitoring and protection
• Smart healthcare
• Decentralized and trustworthy 6G communication infrastructure and solutions
Research Opportunities in the Future
• Internet of Everything
• Data storage and analytics
• Artificial Intelligence
• Vehicle-to-vehicle communication
• UAV
AR
360

FIGURE 2. Architecture diagram of Blockchain in 6G.

1) MASSIVE CONNECTIVITY IN FUTURE SYSTEMS

a: SCALABILITY

Number of devices linked and functioned in future industrial ecosystems are forecasted by industrial IoT enthusiast with the concepts of massive Machine Type Communications (mMTC). Adaption of 6G systems for unprecedented traffic demand remains as a challenging one. Real-time communication is established with less latency. The real-time communication acts as an essential need in the upcoming computing ecosystems. A higher accuracy with zero delay is achieved by D2D and M2M communication for precise operation. AR helped healthcare systems perform delay communication in huge-scale data exchange.

b: HIGHER THROUGHPUT

The decisive systems applied 5G communication ecosystems for providing concurrent connectivity to number of devices. The network organization like base station managed the large number of real time transactions.

c: SYNCHRONIZATION

Synchronization acts as a significant requirement in time vital industrial applications. Efficient operation is attained by the mission critical backbone systems with power allocation systems and vehicular networks harmonized in real time application.

2) SECURITY REQUIREMENTS IN FUTURE COMPUTING ECOSYSTEMS

a: CONFIDENTIALITY AND INTEGRITY

The future computing infrastructure portrayed enormous threat surfaces with wireless connectivity. The encryption methods are lightweight for minimum powered IoT devices. Due to computational restraints, Lightweight cryptographic methods interpret the data into privacy risks. The huge volume of data formed by future systems is required to be accessed and adapted by the legal users during transmission. The eavesdropping and adaptation of data in transmission altered the system operation from expected performance.

b: AVAILABILITY

The service accessibility is the significant requirement in upcoming networks. The superiority of 6G ecosystems with huge volume of interrelated devices prolonged the risk of DDoS attacks.

c: AUTHENTICATION AND ACCESS CONTROL

The federal authentication and access control methods get restrain in huge volume futuristic demands forecasted in 6G. The sophisticated access control required to equal the diversification of future tenants in 6G ecosystem are resource-intensive and origins bottlenecks in associated services.

d: AUDIT

An audit is required to assess the compliance of tenant actions in network ecosystem. Deep packet level audit identifies and flag the tenant behavior for superior security principles. Huge number of tenants auditing remains as a challenging one in security perspective.

3) HIGHER DATA CONSUMPTION IN SOPHISTICATED SOLUTIONS

The higher data rate is an essential prospect in future network ecosystems. The applications like VR, holographic communications, video and 3D ultra-video necessitated enhanced data rate and data utilization.

4) DEVICE RESOURCE RESTRICTIONS

The computational and storage limitations are detected to restrict the abilities of cryptographic methods and caused variation from standard mechanisms. The standard implementation of security is harder with the device resource restrictions.

B. BLOCKCHAIN BENEFITS FOR 6G

Blockchain is an essential technology to allow the potential of 6G systems and address the existing potential demands.

Intelligent resource management: The network resource organization is a challenging one in huge connectivity demands of upcoming telecommunication ecosystems. The resource management functions such as spectrum allocation, orchestration and decentralized evaluation are compatible with the huge infrastructure. Intelligent network framework is applied with the blockchain technology by managing the association among operators and users. Based on game theory, the authors implemented an unlicensed spectrum sharing method. The blockchain and deep reinforcement learning was performed to carry out the resource management services with spectrum allocation and energy organization.

1) ELEVATED SECURITY FEATURES

a: PRIVACY

The privacy is significant in security characteristic. Data privacy application is varied in complex security necessities for 6G network ecosystem. A privacy preserved approach was implemented based on blockchain for content-centric 6G networks.

b: AUTHENTICATION AND ACCESS CONTROL

Access control of centralized systems experienced scalability constraints. The access control with centralization remains as an essential demand in the future networks. A verification and access control approach depended on blockchain was implemented for cloud radio over the fiber network in 6G.

c: ACCOUNTABILITY

The accountability of 6G beyond the network ecosystem is an important requirement. The blockchain and dispersed ledger technology applied security, inspection and authority of network.

III. INTEGRATION OF IoT IN BLOCKCHAIN

An IoT is a diverse available manual method into digitalized description through processing large amount of data. The large data is employed for increasing the quality of life during digitalization process. The development in cloud computing was used for IoT with essential functions. IoT development has new possibility to attain and allocate the data. There is no confidence among the public because they not have clear idea of used data. It makes the developments to IoT through trusted sharing service distribution. The data source is identified at any time and improved the security level. The security is an essential requirement to guarantee that data get shared between available users. A breach in data resulted in the loss of private records and sensitive data. IoT represent network of many electronic devices to communicate with others through open channel. The connection was carried out through wireless technology such as sensor networks, field communication, etc. IoT adjusted the ubiquitous computing with several industrial applications.

Security: When linked device count of network increases, the vulnerability development through external attacks also enhances because of minimum standard device application.

Privacy: The data gathered is broadcasted from IoT devices to cloud storage for processing with third party. The data allocation without the user authority creates data leaks.

Standards: Lack of regulations resulted in undesirable results while organizing the constituted devices.

Latency: The communication principles for various IoT devices caused latency problems. IoT-enabled devices supported the data transmission at higher bandwidth. The devices handled the variations in the configuration like higher bandwidth capacity, increased data-rate and minimal latency.

IV. RESEARCH CHALLENGES OF BLOCKCHAIN WITH IoT ENABLED 6G DEVICES

An IoT and blockchain has large concern from the academic circles and industry. Bitcoin-style blockchain depend on PoW designs with features for many IoT scenarios. With fast development in IoT devices, energy needs are limited. The existing client/server systems are replaced by Blockchain. Information accumulated in nodes is termed as IoT devices. The devices comprise of less computational power and storage capacity to resolve the big hurdle in technology adoption. The research challenges of blockchain with IoT enabled 6G devices are described in Figure 3.

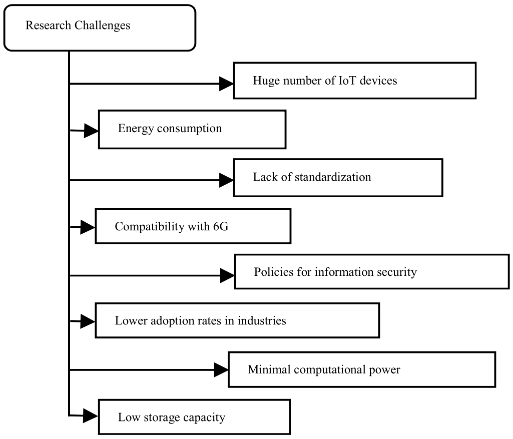
Research Challenges
Huge number of IoT devices
Energy consumption
Lack of standardization
Compatibility with 6G
Policies for information security
Lower adoption rates in industries
Minimal computational power
Low storage capacity

FIGURE 3. Research challenges.

Blockchain gets increased when nodes count in the network increases. There is no equivalence and interoperability where various ledgers not converse with others. The stakeholders are essential one to attain complete interoperability. It required international strategies for collective trust and information security. The firm business cases are not carried out due to the uncertainties. The people are in quandary state of acceptance for industries. It connects different stakeholders in regions without legal compliance. It is demanding for service providers and productions to accept blockchain in diverse business cases. IoT devices are upgraded to the compatible one with high speed network connectivity.

V. BLOCKCHAIN AND IoT INTEGRATION SOLUTIONS

IoT designers had chosen the appropriate solution depending on restrictions and needs. There is no comprehensive analysis and resolutions for IoT manufacturers to attain the appropriate Blockchain platform for integrations. IoT devices required Blockchain to accumulate the state, handle multiple writers and avoid hiring the trusted third party. Block time and transactions per second (TPS) is taken depending on the importance for IoT devices to select the appropriate platform. IoT application has enough knowledge regarding the restrictions and needs like time-sensitivity, transactions and resources. The awareness assisted the IoT devices to describe the proper platform. Scalability, security, privacy and smart capability are the additional metrics that must be satisfied before implementation on IoT devices. A powerful decentralized network was constructed with developer tools for smart contracts, security and contract execution with high level of reliability.

With advanced applications to enhance the superiority of citizen life, IoT acts essential in-service digitization. The access points were used to access and distribute the network information. Centralized data storage systems have contributed for development of IoT. A centralized structure not presented the data transparency. Blockchain technology is an essential resolution to increase the security and privacy. Blockchain can reform the IoT with open, dependence and auditable sharing platform. Figure 4 described the blockchain with 6G-enabled IoT for industrial application.

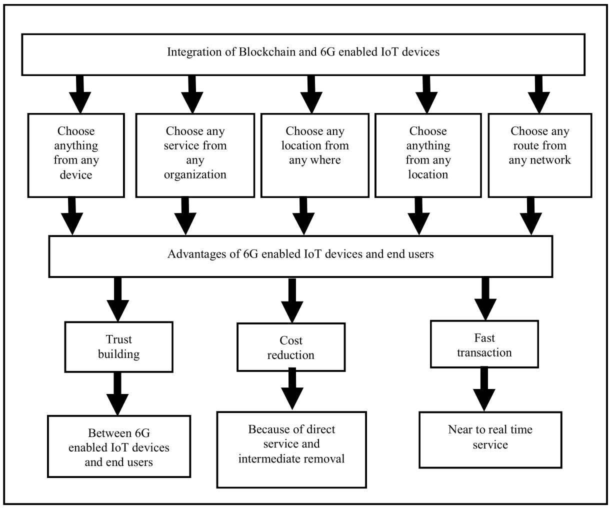
Integration of Blockchain and 6G enabled IoT devices
Choose anything from any device
Choose any service from any organization
Choose any location from any where
Choose anything from any location
Choose any route from any network
Advantages of 6G enabled IoT devices and end users
Trust building
Cost reduction
Fast transaction
Between 6G enabled IoT devices and end users
Because of direct service and intermediate removal
Near to real time service

FIGURE 4. Benefits of blockchain with 6G-enabled IoT for industrial automation.

Decentralization and Scalability: Paradigm shift from the centralized to decentralize for eliminating failure to increase the fault tolerance performance. It restricted the oligarchy of resources where corporations manage gathering and processing of data.

Identity: The common blockchain carried out better identification of every device. The authentication of IoT devices is not provided.

Autonomy: The mobile devices cooperate with each other by means of blockchain to implement the IoT-based industrial applications.

Security: Information exchanges are considered as transactions using new agreements to provide the protected inter-device communication.

Reliability: The incorporation allowed the users for validating the legitimacy of transaction with confidence and responsibility.

Secure code deployment: A manufacturer traced the revise history and allowed them to update IoT devices securely.

VI. APPLICATIONS OF BLOCKCHAIN OF THINGS WITH 6G

A categorization of blockchain- industrial applications in 6G-enabled IoT is described. It comprised conventional sectors of interest for different purposes like smart manufacturing, supply chain management, food industry, smart grid, healthcare, multimedia and digital right management, agriculture and internet of vehicles and unmanned aerial vehicles. Blockchain and 6G increased the security as well as bandwidth with minimal operational and capital expenditure.

The blockchain application for 6G-enabled IoT is described in above Figure 5. The detailed description is given in next subsections.

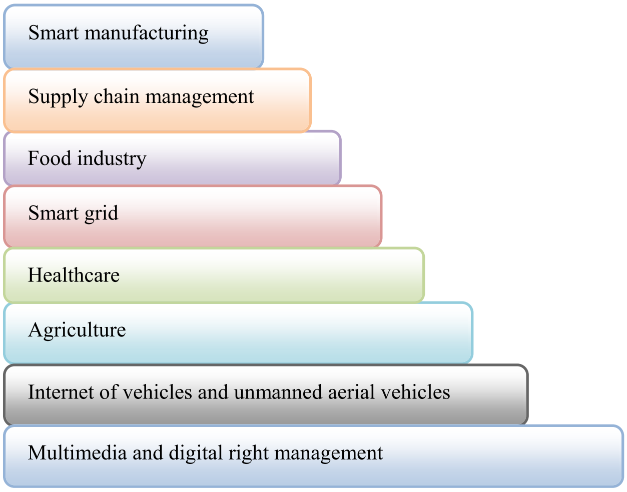
Smart manufacturing
Supply chain management
Food industry
Smart grid
Healthcare
Agriculture
Internet of vehicles and unmanned aerial vehicles
Multimedia and digital right management

FIGURE 5. Applications of Blockchain for 6G-enabled IoT.

A. SMART MANUFACTURING

The manufacturing industry gets upgraded from the automatic to smart technology. Large amount of data is created in each lifecycle phase with product designing, allocation, sell and service. The data get partitioned and resulted in data collection difficulty and data analytics. IoT systems are linked through P2P network for performing the data sharing in industrial sectors and interoperability issues are resolved. BCoT enhanced the security of smart manufacturing.

B. SUPPLY CHAIN MANAGEMENT

A cluster of persons, sources and actions in product lifecycle is termed as Supply chain. It initiates from the creation process to sale process starting at supplier to manufacturer. The supply chain starts with supplier followed by producer, trader, seller and customer as shown in Figure 6.

The process to handle the data and finances when they change by supply chain process is defined as Supply Chain Management (SCM). A product comprised multiple parts presented through different manufacturers across the countries. It is expensive for applying anti-fraud technologies in each product. During blockchain and IoT combination, every part linked with new ID. An immutable timestamp gets connected with ID. The recognition of each part recorded into

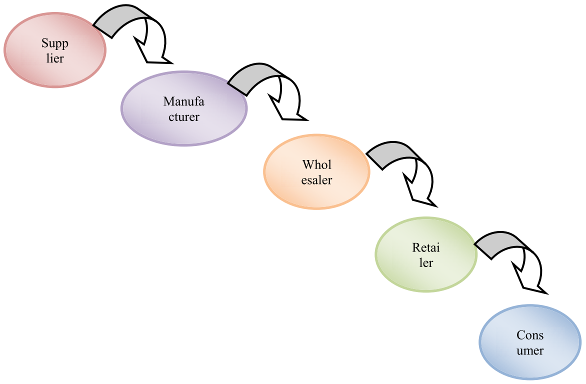

FIGURE 6. Usual flows in supply chain.

blockchain that are tamper-resistant and perceptible. Traceability ontology was introduced with IoT and blockchain technologies depending on the Ethereum blockchain policy to guarantee the data provenance. BCoT minimized the costs in services. The blockchain and IoT integration minimized the cost and risk with high speed. Secured data sharing is attained among different endeavors to improve the customer service by blockchain based machine learning platform.

C. FOOD INDUSTRY

BCoT enhanced the product life cycle in food industry. The traceability of food products acts essential for assuring the food safety. It is a demanding one to guarantee food traceability for IoT. A food company included several of suppliers. The traceability required raw material data from sources for food manufacturing. Blockchain assured the traceability and food industry data origin. RFID and blockchain is employed for launching the supply chain platform from farming for food manufacture in China. The system guaranteed food supply-chain data traceability. Blockchain technology increased the food safety through provision of traceable food products. The combination of blockchain allowed the customers to track food production. Depending on blockchain and IoT tags, a food safety traceability system was introduced. The designed system prevented the data corruption and privacy revelation through smart contracts.

D. SMART GRID

The distributed renewable energy resources appearance alters with energy consumers from pure shoppers to prosumers. Energy prosumers with additional energy trade it to additional consumers. P2P energy trading is the energy between prosumer and consumer. It is a demanding one to ensure the secured energy dealing in distributed atmosphere. The blockchain technology provided opportunities to guarantee the secured P2P energy trading. An energy trading system was introduced depending on consortium blockchains to save cost without broker through blockchains consensus. A decentralized energy-trading system was introduced depending on blockchain for preserving the confidential transaction in smart grid.

E. HEALTHCARE

Healthcare is one of the most important social-economic issues because of population. It included the new demands in healthcare services due to inadequate hospitals. The development in wearable healthcare devices provided healthcare data bring opportunities for providing the remote monitoring services at home. The wearable devices determine and gather the health-care data with heartbeat, diabetes and pressure investigation. With the aid of networks, Doctors access the health-care data at anytime and anywhere. The vulnerability of healthcare devices has many challenges in privacy preservation with higher data security.

The blockchains were integrated into healthcare networks to address the privacy protection of health-care data. The blockchain technology preserved healthcare data stored in cloud servers. The health-care data collected through medical sensors and transmitted to system for patient monitoring. The privacy preservation is carried out in efficient manner. Blockchain was employed to manage the individual healthcare data and to support the data-sharing. Blockchain system ensured the privacy and security of healthcare data. An attribute-based signature method was introduced in healthcare blockchain systems. The designed scheme verified the legitimacy of health-care data and recognition of health-care data owner. Attribute-based signature method improved the privacy level of data owner in healthcare applications.

F. INTERNET OF VEHICLES AND UNMANNED AERIAL VEHICLES

Internet of vehicles (IoV) integrated vehicle to-vehicle networks, vehicle-to-roadside networks, vehicle-to infrastructure networks and vehicle-to-pedestrian networks. The blockchain is integrated with IoV to address the security problems. A trust-management policy was used on blockchains in IoV. Their liability of messages gets authorized through PoW/PoS consensus implemented through RSUs. Blockchain technologies employed to conserve the energy and data communication among electric vehicles and hybrid electric vehicles in smart grids.

G. AGRICULTURE

Smart agriculture employed the new technologies like IoT, GPS and Bigdata for increasing the quantity of agricultural products. Information are stored in control system and examined by AI. The combination of information technologies in smart agriculture makes agricultural supply chain as cost-effective. Distributed Ledger Technologies (DLTs) enhanced the effectiveness, traceability and simplicity in agricultural supply chains. For avoiding the redundant difficulties to accumulate data on blockchain, two associated structure must be designed.

Basic Planting Information: Information regarding specific process of supply chain like production and accumulation is gathered.

Provenance Record: Information regarding agricultural operation is stored.

H. MULTIMEDIA AND DIGITAL RIGHT MANAGEMENT

Media distribution is a category of digital multimedia contents allocation like audio, image and video. The merits of conventional online content delivery medium incorporated enhanced accessibility, cost and higher performance. Due to minimal housing cost, cloud-based Content Delivery Networks (CDNs) are chosen. The designed systems included the inherent problems that are not easy to resolve. Blockchain-based RIGHTs management system (BRIGHT) aimed on video files of blockchain. The existing multimedia failed to conserve any data with respect to ownership or media adaptation records. The original media are tampered for particular purposes to widen the false information over the social media. The watermark comprised information about two characteristics:

Image Hash: It is applied for securing the original media content to get regained when required.

Cryptographic Hash: It comprised transaction record that represents any alteration types to the original media.

VII. CONCLUSION AND FUTURE SCOPE

With fast development in number of connected IoT device, many obstacles occur to minimize the adoption of IoT across different applications. There are many concerns about the interoperability as solutions implemented create the new data silos. The centralized architecture of IoT solution needs the IoT device owners to trust the organizations to maintain the data safe. Blockchain is a promising technology that helped with IoT systems resiliency. A distributed ledger avoided centralized architecture challenges and stores data through its characteristics. Blockchain construct the trust between IoT devices and minimized risk of tampering with Blockchain cryptography. It minimized the cost through eliminating the middlemen and intermediary's overhead. Blockchain provide solution to address many IoT challenges but any convergence between two embedded technologies creates new issues and obstacles. The characteristic of Blockchain gets changed because of IoT requirements like security, data privacy, consensus protocol and smart contracts. Several research papers on Blockchain integration with IoT are reviewed to examine the security issues. From this survey, it is found that the blockchain technology developed for IoT network fails in performance due to more energy consumption, execution time and communication overhead. In some existing works, the data confidentiality and integrity level also remain low. The research challenges and open issues in incorporation of blockchain with 6G communication network are analyzed. Then, the future research guidelines toward blockchain enabled IoT with 6G communication is provided. The future scope of this article is to integrate the blockchain with IoT 6G technologies for reducing the computational cost. Security and privacy issues of 5G technologies are to be reduced depending on demands and requirements.

REFERENCES

[1] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. D. A. Rocha, "A survey of how to use blockchain to secure Internet of Things and the stalker attack," *Secur. Commun. Netw.*, vol. 2018, Apr. 2018, Art. no. 9675050.

[2] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," *Secur. Commun. Netw.*, vol. 2018, Jun. 2018, Art. no. 7817614.

[3] M. Maroufi, R. Abdolee, and B. A. zekand, "On the convergence of blockchain and Internet of Things (IoT) technologies," *Wireless Commun.*, vol. 14, pp. 1–11, Mar. 2019,

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

[5] I. Mistry, S. Tanwar, S. Tyagi, and K. Neeraj, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mech. Syst. Signal Process.*, vol. 135, Sep. 2019, Art. no. 106382.

[6] L. O. Alcaraz López, H. Alves, R. D. Souza, S. Montejo-Sánchez, M. E. G. Fernández, and M. Latva-Aho, "Massive wireless energy transfer: Enabling sustainable IoT towards 6G era," in *Proc. Netw. Internet Archit.*, Dec. 2019, pp. 1–7.

[7] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.

[8] M. Z. Chowdhury, M. Shahjalal, M. K. Hasan, and Y. M. Jang, "The role of optical wireless communication technologies in 5G/6G and IoT solutions: Prospects, directions, and challenges," *Appl. Sci.*, vol. 9, no. 20, pp. 43–67, 2019.

[9] L. Zhang, Y.-C. Liang, and D. Niyato, "6G visions: Mobile ultra-broadband, super Internet-of-things, and artificial intelligence," *China Commun.*, vol. 16, no. 8, pp. 1–14, Aug. 2019.

[10] L. Hang and D.-H. Kim, "Design and implementation of an integrated IoT blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, pp. 22–28, 2019.

[11] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Netw.*, vol. 33, no. 3, pp. 10–17, May 2019.

[12] B.-G. Choi, E. Jeong, and S.-W. Kim, "Multiple security certification system between blockchain based terminal and Internet of Things device: Implication for open innovation," *J. Open Innov., Technol., Market, Complex.*, vol. 5, no. 4, pp. 1–16, 2019.

[13] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Towards 6G networks: Use cases and technologies," *Comput. Sci.*, vol. 58, pp. 1–8, Dec. 2020.

[14] A. K. Biswal, P. Maiti, S. Bebarta, B. Sahoo, and A. K. Turuk, "Authenticating IoT devices with blockchain," in *Advanced Application Blockchain Technology*. Singapore: Springer, 2019, pp. 177–205.

[15] N. Tran, M.-T. Kechadi, S. Pirttikangas, and J. Partala, "Privacy-aware blockchain innovation for 6G: Challenges and opportunities," in *Proc. 6G Wireless Summit*, Mar. 2020, pp. 1–6.

[16] S. K. Singh, S. Rathore, and J. H. Park, "BlockIo T intelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2019,

[17] P. Mendki, "Blockchain enabled IoT edge computing," in *Proc. Int. Conf. Blockchain Technol.*, Marc. 2019, pp. 66–69.

[18] C. Lee, L. Nkenyereye, N. Sung, and J. Song, "Towards a blockchain-enabled IoT platform using one M2M standards," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Nov. 2018, pp. 97–102.

[19] A. Damianou, C. M. Angelopoulos, and V. Katos, "An architecture for blockchain over edge-enabled IoT for smart circular cities," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, 2019, pp. 465–472.

[20] G. Ishmaev, "The ethical limits of blockchain-enabled markets for private IoT data," in *Proc. Philosophy Technol.*, Jun. 2019, pp. 1–22.

[21] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[22] R. Casadei, G. Fortino, D. Pianini, W. Russo, C. Savaglio, and M. Viroli, "A development approach for collective opportunistic Edge-of-Things services," *Inf. Sci.*, vol. 498, pp. 154–169, Sep. 2019.

[23] I. Yaqoob, K. Salah, M. Uddin, R. Jayaraman, M. Omar, and M. Imran, "Blockchain for digital twins: Recent advances and future research challenges," *IEEE Netw.*, early access, Apr. 22, 2020, doi: 10.1109/NET.001.1900661.

[24] F. Miatton, "Blockchain at the edge: The nexus of capturing new value in 5G," in *Proc. Int. Conf. Technol. Entrepreneurship*, Apr. 2020, pp. 1–9.

[25] S. Li, Y. Yuan, J. J. Zhang, B. Buchanan, E. Liu, and R. Ramadoss, "Guest editorial special issue on blockchain-based secure and trusted computing for IoT," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1369–1372, Dec. 2019.

[26] R. Zhu, L. Liu, M. Ma, and L. Hongxiang, "Cognitive-inspired computing: Advances and novel applications," *Future Gener. Comput. Syst.*, vol. 109, pp. 706–709, Aug. 2020.

[27] X. Liu, R. Zhu, A. Anjum, J. Wang, H. Zhang, and M. Ma, "Intelligent data fusion algorithm based on hybrid delay-aware adaptive clustering in wireless sensor networks," *Future Gener. Comput. Syst.*, vol. 104, pp. 1–14, Mar. 2020.

[28] X. Liu, R. Zhu, B. Jalaian, and Y. Sun, "Dynamic spectrum access algorithm based on game theory in cognitive radio networks," *Mobile Netw. Appl.*, vol. 20, no. 6, pp. 817–827, Dec. 2015.

[29] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: A certificate based authentication scheme for smart grid access control," *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[30] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020.

[31] B. D. Deebak and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," *Ad Hoc Netw. J.*, vol. 97, Feb. 2020, Art. no. 102022.