Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7766407

BLOCKCHAIN EMPOWERED CLOUD OF THINGS: A REVIEW ON ITS APPLICATIONS, MERITS AND DEMERITS

Ranu Pandey
Computer Science Research Scholar at Sri Rawatpura Sarkar University, Raipur, Chhattisgarh, IN 492002 (email:ranu_pandey8@hotmail.com)

Dr. Rajesh Kumar Pathak
Vice Chancellor at OPJS UNIVERSITY, RAJASTHAN, INDIA
(email:drrkpathak20@gmail.com)

Abstract—Recently, Blockchain and Cloud of Things (CoT) enabled by the fusion of cloud computing and internet of things have gained prevalent attention due to their tremendous and highly valuable services in modern technical applications. Blockchain provides groundbreaking solutions for confronting network security, data privacy and decentralization challenges in CoT whereas CoT provides scalability and fault tolerance functionalities for strengthening the adeptness of blockchain functions. As both the blockchain and CoT technologies are interdependent, their fusion termed as BCoT serves as a highly promising empowerer for a vast array of use-cases. Therefore, this paper presents an intensive survey of BCoT. It explains the motivation behind blockchain CoT integration. The paper elucidates the scope of collaborating blockchain with CoT and its potential gains. It reviews BCoT applications in heterogeneous use-case domains. This article presents various merits of blockchain CoT integration. It then identifies and describes the critical research barriers and open problems along with prominent solutions. Lastly, this survey provides significant further directions for promoting research studies in this field.

Index Terms— Blockchain, BCoT integration, Cloud of Things, Commercial applications

I. INTRODUCTION

RECENTLY, blockchain technology has received immense attention in applications requiring decentralized and enhanced security features. The swift advancement in the exploitation of blockchain is clearing the path for future generation and budding commercial and financial service realms. This inturn is influencing miscellaneous facets of human lives in diverse ways. Blockchain typically is a distributed, public and immutable database employed for securing various transactions. This technology mainly relies on a peer-to-peer (P2P) system architecture wherein the transaction data is controlled decentrally and not by any centralized entity. The transaction details in blockchain are stored in a series of blocks which are accessible publicly to all blockchain network participants in a credible manner. The legitimacy of transactions are validated through cryptography and consensus mechanisms in blockchain for ensuring resistance of connected blocks against alterations and modifications [1]. This technology also provides transparency, immutability and security along with decentralization which boost the service efficacy. These outstanding properties have encouraged the adoption of this technology and its implementation in diverse sectors nowadays.

In addition to blockchain, other technologies ruling the world these days are Cloud Computing (CC) and Internet of Things (IoT). IoT typically is a network of physical things which can be controlled or monitored through ubiquitous electronic components for facilitating smart industrial services like smart cities, smart manufacturing, smart industries, etc. This technology has empowered the object with the capability to communicate and connect via the internet, thus bridging the digital and physical worlds, whereby information can be collected and disseminated into massive networks at the high range of granularity. But the constrained resources of IoT gadgets have devolved the IoT application tasks to CC thus giving rise to Cloud of things (CoT) epitome [2], [3]. Through CoT a strong, flexible CC environment can be provided for handling IoT services, presenting tremendous possibilities for boosting the efficacy and performance of services [4]. But the classical CoT infrastructures have become ineffective because of the following issues. Firstly, the classical CoT solutions mainly rely on centralized frameworks for IoT service operations that make it extremely tedious to scale in case of massive or huge IoT networks [5]. Secondly, many CoT systems behest third party trusting for IoT information processing, which may raise severe information privacy problems. Lastly, the centralized system infrastructure may cause the IoT devices to suffer high power consumption and communication latency issues owing to the distant information transmission, thereby impeding the widespread distributions of CoT in realistic scenarios [6].

For achieving a sustainable growth of CoT and replacing the centralized computing frameworks, constructing a highly decentralized ecosystem has become crucial in present-day applications. As blockchain is a robust candidate for realizing the complete decentralization of CoT systems, the collaboration of blockchain and CoT known as BCoT can bring huge profits to industries and communities. This new paradigm (BCoT) combining the advantages of both CoT and blockchain can create wonders for emerging applications in diverse manners. Through offering a decentralized storage platform using virtual storage, BCoT can facilitate entirely new cloud storage operations that are highly resistant to information modifications. Rather than relying on conventional data centres of cloud, BCoT can interconnect virtual machines and external computers on cloud for constructing a completely decentralized storage network without requiring any central authority. This BCoT concept can resolve many other problems encountered by standalone CoT or standalone blockchain systems. Moreover, BCoT can provide numerous potential benefits like high privacy, improved security, better cooperation, decentralization, fault tolerance and scalable support for transactions.

A. Related Studies and Contribution of the Paper

Various studies in CoT, blockchain and related topics have been probed over the past years. Numerous efforts have been done for providing survey works in these research areas. The review works [7], [8], [9] provided the survey of recent attempts in the utilization of blockchain platforms in different IoT applications and scenarios. In [10], consolidation of blockchain with IoT was discussed. The prime interest of the study was the inspection of blockchain capacity for heterogeneous IoT applications stretching from intelligent manufacturing to smart vehicles, drones and communication networks (5G networks). In [11], a study discussing the utilization of blockchain for offering security services was presented. It also described the technical characteristics of blockchain for settling the difficulties in heterogeneous application areas, including cloud computing and IoT. In [12], the technical notions of blockchain like the inherent concepts, consensus and networking strategies were elaborated. In [13], the integrated framework of edge computing and blockchain was discussed. In [14], the technical problems, opportunities and challenges linked with consolidation of cloud computing and blockchain were studied.

Although CoT and blockchain have been extensively studied in the literature, just a limited amount of studies provide a thorough review on the collaboration of these vital research areas. In comparison to afore-discussed research studies, in this survey, a comprehensive review on the collaboration of CoT and blockchain is provided with a broad discussion on several aspects. The ultimate objective of this review is to offer readers with deep knowledge of CoT and blockchain integration. The prime contributions of this paper are featured as follows:

1) To present a state-of-the-art review on the collaboration of CoT and blockchain with a widespread discussion on distinct technical concepts like BCoT background, motivation for the integration of CoT and blockchain and the benefits of the collaborated framework.
2) To explore the diverse applications of BCoT in different sectors and to analyze its benefit.
3) To determine the significant technical hardships, open problems persisting in this field and to explore the further research directions for extending the BCoT scope in looming applications.

B. Paper Organization

This review paper is arranged as shown in Figure 1. Section II provides the background information of CoT and blockchain and highlights the motivations for BCoT integration. Section III discusses the diverse applications of BCoT in various fields. Section IV discusses the opportunities of BCoT with regard to different factors. Section V describes the open issues and the possible technical challenges in BCoT collaboration. Section VI provides some insights on convergence of BCoT with other emerging technologies and discusses the future directions of integrating BCoT with such technologies. Section VII concludes the work.

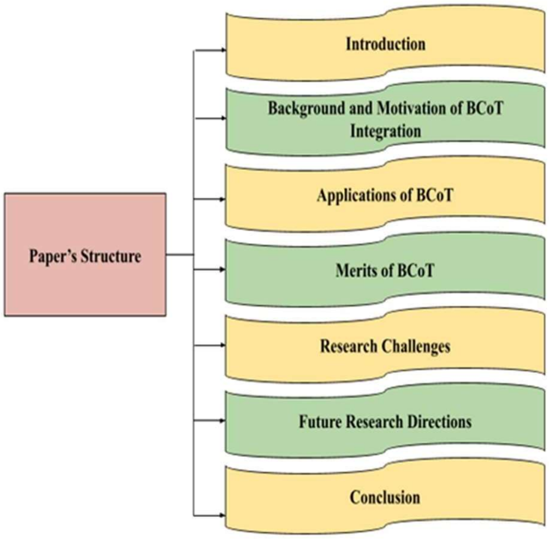

Fig. 1. Structure of the Review Paper

II. BACKGROUND AND MOTIVATION OF BCOT INTEGRATION

The background information of CoT and blockchain is presented in this section and the motivations for the integrating these technologies is provided.

A. Blockchain

The blockchain is generally a public, shared and trusted ledger based on a P2P network. In blockchain every node possesses the chance of verifying the other entity's actions for creating, validating and authenticating the fresh transaction to be recorded. This decentralized structure guarantees secure and robust operations with the benefits of no one-point failure and tamper resistance vulnerabilities. Blockchain network is typically constructed using some prime components like data block, smart contracts, distributed ledger and consensus. Every data block comprising numerous transactions is connected to its neighboring block via a hash function. All these blocks can be tracked and therefore no alteration or modification can be done to the data block. Distributed ledger basically is a kind of database that is replicated and shared among the participants of a P2P network. The consensus is a procedure employed for performing agreement on an individual block among several unreliable nodes for assuring security in the blockchain system. Lastly, smart contracts are programmable applications running on the network as per predefined contractual terms such as license, confidentiality and payment conditions. The decentralization feature of blockchain brings promising advantages including operational cost saving, elimination of single point damage risks and improved trustworthiness. Another significant characteristic of blockchain is transparency which arises from the notion that all transaction data is viewable on blockchain to all participating network entities. Consequently, all blockchain participants/users can completely access, validate and trace transaction activities on the network.

B. Cloud of Things (CoT)

IoT these days is becoming a fundamental segment of almost every automated application and is obtaining growing attention from industries and academics. It seamlessly interconnects miscellaneous objects and devices for setting up a physical platform wherein processing, sensing and interacting actions are intelligently implemented without manual intervention. However, enormous chunks of information produced from a vast range of devices in present IoT systems has become a strangulation in ensuring the needed service because of inhibited storage resources and power of IoT tools. Nevertheless, the unconstrained resources of CC in terms of computation power and storage volume can offer on-demand, efficient and strong services for IoT usage fields. Moreover, the consolidation of CC with IoT has prepared the ground for a fresh epitome like CoT capable of empowering both CC and IoT domains. Indeed, the abundance of resources existing on cloud are largely useful for IoT systems and additionally cloud can obtain more stardom in real-world applications through integrating it with IoT. Through CoT the present IoT service provisioning frameworks can be transformed with high service availability, ameliorated system performance and reduced management effort. The CoT can deliver immediate services to its users anytime and anywhere. Moreover, with unconstrained virtual processing abilities of CC, CoT can open fresh opportunities for improving IoT computation through remotely executing data and facilitating data offloading leading to not solely computation improvement but even addressing bandwidth preservation and energy conservation problems of IoT components. Significantly, CoT can provide automatic and simplified solutions through exploiting virtual machines, resource infrastructure and cloud servers. Moreover, the facility of system management frameworks existing on clouds supports boundless interconnections and communications between users, things and IoT devices for empowering pervasive applications.

C. Motivation of BCoT Integration

The diverse security issues (such as data availability, data integrity and privacy management) of CoT and technical weaknesses (such as security flaw and complexity) of blockchain are the prime motivations for integration of CoT with blockchain.

1) Security concerns in CoT:

In the present cloud architectures, as the cloud services are managed centrally through the centralized authority, they are prone to single-point failures, introducing threats to the cloud service availability for on-demand access of IoT. Moreover, these centralized cloud IoT networks fail to ensure uninterrupted provisions of services when several users simultaneously request data and when cloud servers are devastated by cyber-attacks or software bugs. These data availability challenges motivate the integration of a decentralized framework with CoT. The analysis and storage of IoT data on clouds often introduce integrity concerns. The outsourced data faces risks of being deleted or modified without user approval by third parties. Moreover, tampering of cloud information resources by adversaries for their personal benefit can violate data integrity. Several public verification methods employed for addressing the data integrity problems, raised several concerns, including invalidated verification owing to hostile auditors. These data integrity concerns promote exploitation of new solutions for CoT networks.

2) Technical weaknesses of blockchain:

Despite offering many useful services, blockchain still faces certain hardships with respect to security flaw and complexity. In IoT systems, IoT devices serve as blockchain entities for running the consensus procedure for resolving the tedious mathematical operations, which require robust computation hardware. Miserably, the IoT resource bounds make it challenging to satisfy such requirements. Also in IoT components with proportionately large computing capacities, executing complex blockchain procedures may need intensive resources which may raise user concerns regarding huge operational expenses, thereby impeding the widespread dissemination of blockchain-based networks. These problems encourage the utilization of better frameworks for overcoming complexity challenges of blockchain. Another limitation of modern blockchains include ineluctable security flaw. In case of multiple computers serving as blockchain nodes for controlling computing power, malicious attackers may tamper consensus frameworks and prevent fresh transactions from receiving assertions for malicious access. Blockchain can suffer risks of system hazards and information breach without a global transaction management.

These security concerns of CoT and technical bounds of blockchain encourage the integration of CoT and blockchain, thus introducing the BCoT architecture. Concisely the utilization of cloud resources in CoT by blockchain can provide reliable information storage and rigorous mining computations while the CoT decentralization can address the privacy and security issues.

III. APPLICATIONS OF BCOT

This section discusses the chief BCoT applications over diverse domains including smart healthcare, intelligent resource management, smart transportation, smart industry, smart education, intelligent cloud services and smart city.

A. Intelligent resource management

Automated resource management in BCoT is receiving extensive attention these days. BCoT provides persuasive resource management coupled with a vast array of provisions on resource-intensive operations, real-time processing, consensus process and blockchain mining. Through smart contracts existing on blockchain [15] in BCoT, resource management mechanisms can gain truthfulness, high transparency and ensure strong access control within collaborative systems of customers and resource providers.

B. Smart education

Application of BCoT in the educational realm can offer multitudinous benefits. It can aid in securely sharing and validating the learning databank of academic or educational institutions, students' personal details and academic certificates or achievements [16]. CC and unalterable blockchain ledgers can aid in developing trusted and secure educational platforms for fostering educational collaboration.

C. Smart city

Advances in IoT and CC have given birth to novel epitomes like smart city for dynamically utilizing the diverse resources in urban regions and delivering a broad degree of services to citizens. Typically, smart cities encompass multiple components including widespread information storage, heterogeneous networks, pervasive IoT devices and robust processing centres like CC for service facilities. Despite the latent prospect of smart cities, providing secure, efficient and better smart city-enabled services remains a tough challenge. Under this setting, BCoT can furnish attractive solutions for empowering smart city operations by exploiting innovative technical attributes of blockchain and CC [17], [18]. Moreover, it can endorse global connectivity between industrial applications and citizens. Integration of CoT and blockchain can reshape smart city configurations to confront barriers in system performance and security.

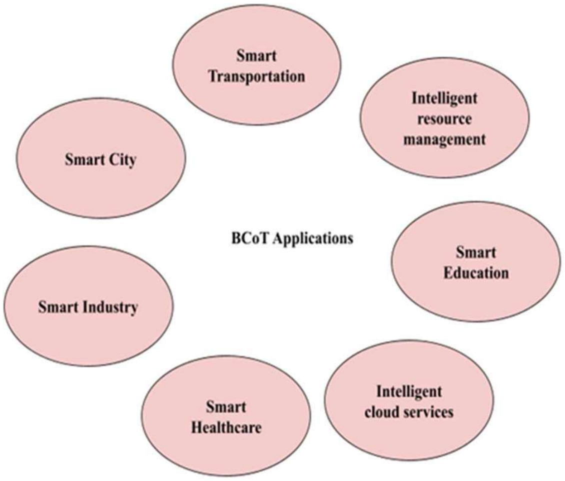

Fig. 2. BCoT applications

1) Smart homes:

Home automation renders a new dimension to smart city context. Smart home basically is a system of IoT components configured using intelligent sensors, automated devices and detectors that gather data from the environment. Despite major potencies to benefit people, smart homes experience impediments in security, data privacy and attacks. For confronting these weaknesses, utilization of BCoT platforms can offer favorable solutions [19]. BCoT can empower smart services like access control, home management and user monitoring in automated home scenarios. Moreover, BCoT can make transaction processing and information storage more resilient and safe among IoT components, external users and home owner.

2) Smart city security services:

The ubiquitous characteristic of information-based services make smart city frameworks to experience security bottlenecks like trust, privacy, integrity, etc. [20]. The BCoT framework with elevated security capabilities helps to combat such hurdles and offer promising smart city security services. Indeed, it provides critical cryptographic primitives like authenticity, integrity, non-repudiation and confidentiality through constructing decentralized security configurations for smart cities. Moreover, implementation of BCoT in smart city domain can offer finest security services. CC can provide robust computing capacities for managing bulky IoT information streams and improved security attributes of blockchain can control smart city tasks in a safe and decentralized manner.

D. Smart healthcare

Generally, healthcare is a commercial sector wherein medical institutions and organizations offer healthcare services, medical insurance and medical equipment for providing required healthcare facilities to its patients. In the healthcare realm, use of BCoT frameworks can endow great potentials for resolving service efficiency and security issues. Moreover, through exploiting these frameworks medical services and clinical operations can be further enhanced [21], [22], [23], [24]. BCoT technology in healthcare vows to offer automated services like health information storage, health or medical data sharing and safe service management in healthcare [25], [26], [27], [28], [29].

1) Health information storage

In classical IoT cloud-oriented health systems, clinical data is generally stored in CC under the control of cloud SPs. In these health systems, confidential patient information may be prone to data leakage hazards owing to curious behaviors of cloud SPs. Additionally, the transfer of EHRs to the cloud can even be susceptible to heterogeneous attacks on information storage despite security tools of CC. In such contexts, robust security potentials of blockchain can ameliorate the safety and efficacy of health information storage. Exploiting BCoT platforms, encrypted health documents can be preserved in blockchain cloud via smart contracts and complete data integrity can be assured to health data users and patients. Vulnerabilities concerning information storage can be effectively addressed through employing cryptographic operations along with improving accountability, security and integrity of storage [30].

2) Medical data sharing

In this digital healthcare era, heaps of electronic healthcare records (EHRs) are generated and shared between patients and health organizations for supporting data analysis, decision making and accomplishing widespread healthcare delivery. Particularly, CoT provisions effective medical data sharing scenarios wherein EHRs can be effectively processed and preserved on cloud systems. Users can acquire their health data through mobile gadgets like smartphones for health status monitoring. Furthermore, it promises to achieve healthcare services on-demand and healthcare cost saving [31]. But dynamic IoT-cloud platform based healthcare information sharing is often susceptible to privacy and safety hazards because of attack possibilities and mistrust between users, healthcare cloud storage and cloud providers. In this vein, blockchain aids in fixing security hurdles in health information sharing through decentralized health information authentication of all involved peers and data verification via consensus mechanisms. The blockchains traceability feature enables medical entities (i.e. patients, healthcare providers and insurance organizations) to trace effectively the user access activities and identify data threats, aiming to strengthen the health information sharing security in BCoT systems. Exploitation of BCoT architecture in health information sharing, aids in safeguarding medical data through securely storing EHRs in the cloud and data indexes in blockchain, thereby ensuring no arbitrary alteration of EHRs [32], [33], [34]. Despite BCoT aids in securing information sharing, the repositioning of all medical information on blockchain can hamper transaction functions and put confidential patient data at hazards of information leakage. Therefore, through encrypting massive health databases, storing them in off-chain mode in cloud and storing only hash values or metadata of raw information in blockchain can surmount the size constraint of the whopping data storage or information preservation in BCoT arrangements [35]. Furthermore, through tracing data access activities of users and exploiting cryptographic approaches for authentication while data sharing can further boost the health information sharing security [36], [37].

3) Smart service management

BCoT can render unconventional breakthroughs with novel intelligent medical services like healthcare operation control or safe user management, decentralized healthcare, etc. [38]. It can aid in developing a safe healthcare communication ecosystem among healthcare users, device suppliers and purchasing managers under the supervision of smart agreements for access authentication and data traceability [39]. Moreover, BCoT frameworks in healthcare operations can offer strong healthcare computing services like storage and smart computation. They are effective in upgrading the medical service quality including healthcare remedy assessment, patient diagnosis and health monitoring [40].

E. Smart industry

BCoT has appeared as a key technology for driving smart industries. It promises to entitle industrial settings with improved operation efficacy and enhanced security. The vital smart industry applications include smart supply chain, smart manufacturing and smart energy.

1) Smart supply chain

BCoT is beneficial to commercial supply chain which is the pivotal segment of the general smart industry environment. In fact, BCoT with robust immutable and decentralized attributes of blockchain can assure more efficient, secure and faster corporation between users, manufacturers and industries in logistic and supply chain activities [41], [42]. Moreover, it can even facilitate secure monitoring, support planning and scheduling supply chain functions. In BCoT, CC can offer numerous flexible operations for blockchain-oriented supply chain while blockchain can guarantee trust among businesses and companies during supply chain functions via smart contracts and consensus mechanisms. Information privacy and security during these functions can be ensured through consensus methods across the P2P network enabled through cloud-blockchain fusion.

2) Smart manufacturing

Basically, smart manufacturing employs IoT enabled methods, service-directed manufacturing and cloud-based schemes for boosting the manufacturing performance. However, existing models still experience complications related to third party-enabled authority and centralized network control. In short, centralized manufacturing infrastructures face constraints like low security, flexibility and efficiency. Therefore, in manufacturing domains, utilization of BCoT can assist in confronting such crucial hardships. Furthermore, BCoT can optimize and enhance manufacturing operations and curtail operational costs [43]. Specifically, it can boost the security of manufacturing processes through offering effective security facilities for privacy and trust establishment among diverse manufacturing enterprises. Moreover, customers and SPs can share desired information and business-pertinent data over the BCoT network with guaranteed security. Smart contracts in the manufacturing domain serve as accords between manufacturing resources and service consumers for providing requested manufacturing services [44]. Altogether, BCoT can enhance the smart industry performance through ensuring lower operational expenses, efficient manufacturing and reduced management efforts by utilizing service assistance of CC, security and controlling potentials of blockchain.

3) Smart energy

Smart energy persists to retain a critical position in industrial ecosystems due to augmenting energy usage demands for supporting manufacturing and industrial tasks. The energy plant's overall purpose is to offer cost efficient, sustainable and reliable energy services to industries and customers. Existing energy systems often experience security problems during energy trading. BCoT architectures in these situations appear as promising countermeasures. BCoT empowered with immutable blockchain can strengthen the privacy and safety of energy trade and transmission [45], [46] while BCoT empowered with CC can offer energy management and storage services along with supporting blockchain in accomplishing decentralized energy functions.

F. Smart transportation

Smart transportation system (STS) have witnessed terrific growth recently owing to drastic advancement of current sensing, computing, and communicating technologies. Smart transport networks impose pivotal impacts on diverse facets of human lives with intelligent transport services, vehicles and facilities. Being a vital IoT application, smart transportation faces security hazards owing to vehicle-to-vehicle interaction in non-trusted vehicular settings. BCoT possesses the ability to create a trusted, decentralized and secure STS ecosystem. The fusion of blockchain with elevated security features and CC with unlimited data management potential can enhance service quality and security in STS, including safe vehicular services and vehicular communication control [47], [48], [49].

1) Secure vehicular operations

The traceability and decentralization attributes of blockchain can facilitate safe vehicular services like task scheduling, vehicular report, trust control, data carpooling and insurance management [50], [51], [52], [53] while CoT provides a new category of automotive services with finer security and efficacy. The consolidation of CoT and blockchain (BCoT) can open up neoteric opportunities for promoting vehicular services, which vow to transform STS.

2) Vehicular communication control

In vehicular communication control, blockchain is employed in energy and information interaction processes for achieving data confidentiality via cryptography and user authentication via smart contracts. Blockchain allows to form a safe P2P network for facilitating perpetual communications among pervasive vehicles for collaborative trust, service management and value exchange [54], [55].

G. Intelligent cloud services

CC offers numerous outsourcing services like computation and storage for serving organizations and individuals. These outsourcing services generally face security and online payment problems. As many conventional service solutions depend on trusted third party for achieving fair payments, realization of reasonable and secure costs of outsourcing services is really substantial for cloud-oriented applications [56]. From this outlook, BCoT appears as a robust candidate for fixing security impediments of cloud functions and simplifying service management. BCoT architecture offers an immense potential for transforming cloud-directed services with improved protection and efficiency levels. Moreover, it can assure trustfulness, data availability and integrity through smart agreements and consensus techniques. Significantly, it can provision decentralized cloud functions with benefits over classical cloud ecosystems for less communication overheads and better robustness.

IV. MERITS OF BCOT

The integrated CoT and blockchain framework offers numerous advantages including improved security, decentralization management, enhanced data privacy, cost saving, fault resilience, scalability, enhanced processing speed and minimized system complexity.

A. Improved security

Blockchain offers solutions for enhancing the CoT system security through providing significant security characteristics like availability and confidentiality. All records in BCoT systems are hashed cryptographically and transactions are authorized by participants such that all interactions with cloud are maintained confidential under blockchain-directed signatures. The decentralized characteristic of blockchain allows data replication across all participating entities and therefore BCoT assures improved availability. Moreover, the resourceful CC can offer off-chain storage facilities on the interruption of the core BCoT network owing to foreign attacks for supporting the on-chain storage system's data availability. Implementation of blockchain techniques on clouds can also boost the blockchain systems' security. For instance, clouds can utilize their existing network security techniques for preserving and maintaining the blockchain software.

B. Decentralization management

Inspired by the completely decentralized property of blockchain, a decentralized BCoT architecture can be built under the disseminated control of the P2P network of IoT devices and cloud nodes. Using decentralized consensus, identical copies of information records can be maintained by blockchain peers and distributed uniformly among the participants. Through this decentralized structure, one point failure impediments can be completely eliminated, interruption of BCoT operations can be efficiently prevented and data availability can be largely enhanced.

C. Enhanced data privacy

The information exchange between IoT devices and cloud providers and the dynamic procedure of outsourcing information to clouds are susceptible to data leak and attacks by third parties or adversaries. In these situations, the transparency, integrity and immutability properties of blockchain are eminently suitable for defending the information in CoT systems. Since blockchain is controlled by immutable and safe consensus mechanisms any alteration of records or tampering of information is utterly impossible in realistic environments. Consequently, blockchain properties largely boost the information privacy for diverse BCoT applications.

D. Cost saving

Available IoT solutions generally are expensive owing to high maintenance and infrastructure expenses associated with networking equipment, centralized architecture and large servers. Utilization of cheaper configurations for handling cost issues in such applications often result in security compromisation. Therefore, exploitation of alternative platforms like BCoT which can assure both cost savings and security because of its decentralized, resilient and immutable nature can hugely benefit IoT applications.

E. Enhanced processing speed

The colossal data processing difficulties encountered in heterogeneous IoT applications can be resolved through exploiting BCoT architecture. The decentralized property of blockchain and the cloud's capability of arranging on-demand computing resources in BCoT greatly enhances the processing speed.

F. Scalability

In massive blockchain networks, the amount of transactions may be more owing to involvement of various processes. The numerous transactions involved can retard the processing velocity of blockchain systems. Therefore, it is incredibly important to offer robust information processing services for accelerating transaction execution and facilitating scalable blockchain operations. However, utilizing the blockchain method alone is not feasible for achieving scalability. But integration of CC with blockchain can provide desired scalability. Thus BCoT architecture comprising both blockchain and cloud can satisfy scalability requisites of applications.

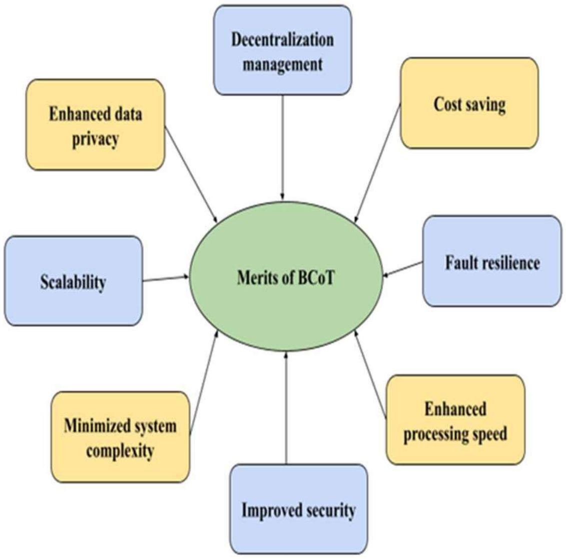

Fig. 3. Merits of BCoT.

G. Fault resilience

BCoT can aid in replicating blockchain information across numerous computing servers that are strongly interconnected through collaborative clouds. This can curtail the one-point failure hazards owing to cloud node disruption and guarantee ceaseless services. The inter-cloud mechanism can facilitate blockchain network to function perpetually even if a cloud server is being attacked.

H. Minimized system complexity

Through integrating CC with blockchain, BCoT can decrease the system implementation complexity. This integration allows to operate the blockchain for different BCoT projects without bothering about inherent hardware technologies. Besides, blockchain algorithms can be executed online through exploiting cloud infrastructure which are promising in minimizing resource expenses for executing or running blockchain. Furthermore, the fusion of CoT and blockchain create many opportunities for deploying BCoT networks on a wider range with cheap and simple implementations.

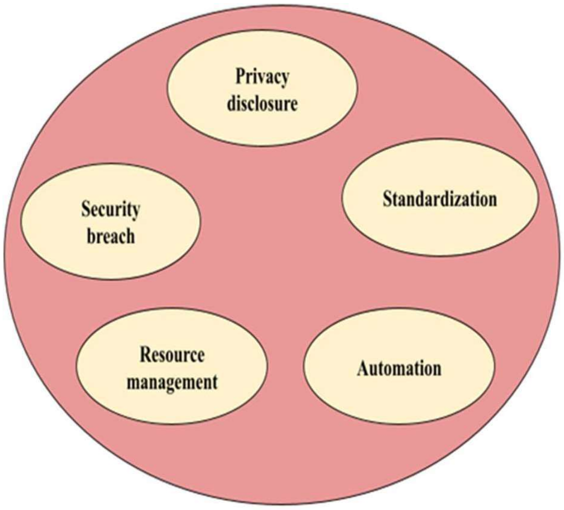

Fig. 4. Main challenges

V. RESEARCH CHALLENGES

In BCoT systems, the key challenges include privacy disclosure, standardization, resource management, intelligence and security breach.

1) Privacy disclosure

In present BCoT systems, information can be preserved off-chain in cloud storage for diminishing the overload on blockchain. Nevertheless, this storage framework can create additional privacy concerns. Utilization of a stand-alone entity as a network participant for legitimately performing cloud information processing may also obtain personal data without the users' consent thus causing severe data leakage problems. Consequently, external attacks may also acquire malicious access for retrieving cloud information or modifying and illegally altering the outsourced IoT archives on cloud. Another crucial problem can be privacy disclosure on blockchain transactions. Though blockchain exploits digital signature and encryption for preserving transactions, a certain quantity of transaction details may leak amid blockchain operations. Therefore, from a practical standpoint information security of blockchain is not highly robust. Besides, criminals can utilize smart contracts for illicit purposes, leading to confidential data leakage and theft of secret keys. Significantly, user privacy in BCoT cannot be fully guaranteed because all user data like amount values, receiver and sender addresses are publicly available on communicating network owing to the blockchain's transparency property. Thus attackers or malicious users can examine such data and maintain records of participants' activities, which can end in disclosure of personal data.

2) Standardization

From its commencement, the blockchain has revolutionized companies or commercial sectors through providing new network frameworks with its secure and decentralized properties. Furthermore, it has the power to transform the current trend of CoT businesses and reform commercial network architectures with improved BCoT paradigms. Though the unification of CoT and blockchain can provision multiple gains to IoT systems, the BCoT paradigm has been developed presently without standards and hence is constrained to only certain service providers (SPs). Consequently, every SP predominantly develops and provides BCoT for particular purposes rather than general designs which are applicable for heterogeneous use-case regimes. The distinct operational hypothesis, diverse service definitions and distinct network management concepts have been deemed as the key rationales for lack of standard. The inadequate system standard has restricted the possible collaborations between SPs, thereby making the customers to experience troubles in changing their SPs. Additionally, non-standard diverse communication protocols between heterogeneous CoT systems and blockchain platforms have further complicated the procedures for widespread BCoT deployments.

3) Resource management

For achieving flexibility, cost reduction and sustainable profit gain in cloud service, the effective resource management is tremendously significant in BCoT and therefore requires high research efforts. Indeed, for effective resource management in BCoT, strong and adaptive models are needed for fixing several technical issues from resource assignment, bandwidth reservation to workload allocation and task allocation. As the resources are segregated for serving multiple intents including use of some resources for meeting user demands and some others for maintaining blockchain, these issues turn more complicated when integrating CC in blockchain. Thus innovative ideas are much-desired for tackling these hurdles with regard to resource management in coordinated BCoT networks.

4) Automation

BCoT systems currently are mainly employed for security services, data sharing and data storage. However, limited research interest has been given to incorporating intelligent services along with existing facilities in BCoT applications. The intelligent services like automated data analytics, automated decision making mechanisms or smart management tools are having greater demands in current industries for enabling better service delivery to users. For instance, a smart traffic analytic system in cloud-oriented vehicular networks can assist vehicle drivers in route change for minimizing the chances of congestion. Further, a smart medical support mechanism based on CC in medicare can make treatment and diagnosis much simpler. These automated services in BCoT-directed applications are productive in enhancing system efficacy and in fulfilling quality of user experience. Thus automation in BCoT is deemed as a critical open problem where more research initiatives are strongly required.

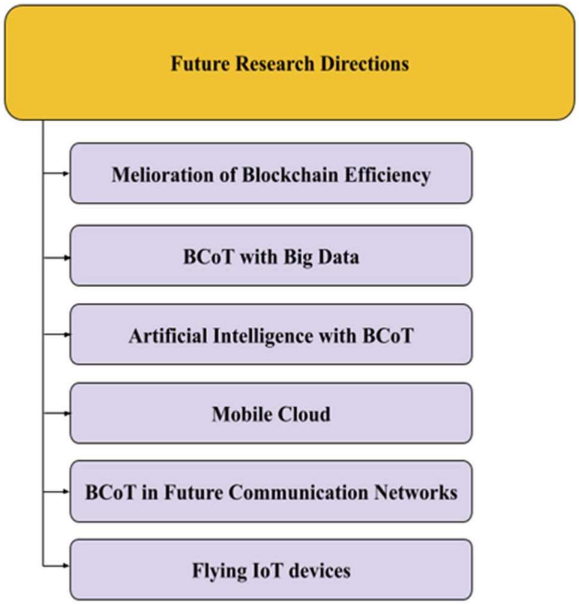
Future Research Directions
Melioration of Blockchain Efficiency
BCoT with Big Data
Artificial Intelligence with BCoT
Mobile Cloud
BCoT in Future Communication Networks
Flying IoT devices

Fig. 5. Further directions of research

5) Security breach

Despite security benefits (like encryption, verifiability, decentralization and immutability) offered by blockchain to CoT, security problems in BCoT still continue because of the susceptibilities of both blockchain and CoT systems. The rising need of IoT data outsourcing to clouds in CoT for computation and storage services has created innumerable fresh challenging security problems including access control, system integrity, identity management and authentication [57]. Furthermore, various vital security attacks in CoT like adversarial IoT attacks, eavesdropping, degraded connection quality and unsecured communication mediums have added high security threats to CoT systems. Cloud services developed for BCoT systems also experience DoS and malware injection attacks, virtual machine transfer attacks and severe other security risks [58]. These security bottlenecks can prevent fresh transactions from obtaining confirmations and even impede payments between IoT users and SPs. Moreover, attackers can use this vulnerability for initiating dual spending attacks or hampering usual mining operations and altering the sequence of transactions, all of them leading to blockchain network degradation [59]. Additionally, the security prospect of smart contract is also vitally significant since a tiny bug can evoke serious problems like system logic tampering or privacy disclosure [60], [61]. Some of paramount security threats can include reentrancy attacks, timestamp dependence and mishandled exceptions on smart agreements in BCoT implementations.

A. Solutions

Various BCoT SPs must perform a service contract on the inclusion of CoT and blockchain. Technical aspects namely blockchain deployment, service payment methods, IoT device consolidation and network settings should be cautiously considered. Affiliation of SPs can be supportive in standardizing BCoT technology. The simultaneous development of global BCoT standards among multiple SPs in customer service assistance and blockchain cloud design can facilitate more BCoT-related organizations [62]. Furthermore, security hurdles in BCoT can be settled through security upgrades in both CoT and blockchain networks. From CoT perspective, security assessments and befitting solutions are extremely predominant [63]. Efficient security evaluation tools for investigating, preventing threat possibilities and guaranteeing trustful smart agreement implementation on blockchain can contribute towards addressing security concerns in BCoT scenarios and enhancing the overall system performance [64]. Moreover, utilization of several innovative approaches like improved user identification, encryption techniques, intention hiding methods, access control and trusted CC can further boost the privacy of BCoT systems [65]. From a blockchain perspective, anonymity acts as a critical entity in ensuring strong privacy. Hence, user data can be efficiently hidden on blockchain, through avoiding attackers from guessing the identity of involved transactions and thereby preserving private user data. Also the adoption of intelligent tools and expert systems can be a right solution for providing automation in BCoT-oriented applications. For effective resource management, exploitation of intelligent energy-conscious resource management frameworks and machine learning embedded with smart contracts can optimize resource management as per user demands. This inturn can assist cloud SPs to gain vast profits.

VI. FUTURE RESEARCH DIRECTIONS

The vast attention gained by BCoT from industries and academics has augmented the space for integrating other technologies with BCoT. Convergence of these technologies and BCoT can open multiple opportunities for emerging applications and services. This section presents glimpses of future research opportunities with regard to integrating BCoT with enabling technologies.

A. Melioration of blockchain efficacy

For acquiring the maximum benefit of the blockchain paradigm in emerging BCoT applications, enhancing the blockchain performance has become terribly important. Because of the blockchain's security attributes, user messages must be authenticated and transactions should be verified by every blockchain node. This may require enormous storage and computing resources. It also needs energy resources and network bandwidth for implementing the mining procedure. Present blockchain designs also suffer scalability problems from the viewpoint of networking, storage and throughput. For instance, many present blockchain designs utilize long duration for processing transactions owing to constraints like block size, network traffic, etc. Additionally, every blockchain node frequently has to preserve a replica of entire transaction information which creates a storage load on the blockchain. The consolidation of blockchain with CoT can thus introduce fresh technical hurdles which can unfavorably affect the BCoT system performance. Recently, researchers have come up with several solutions for tackling these hurdles. Through designing efficient block validation methods [66] or constricting consensus storage [67], blockchain performance and its efficacy can be improved. These approaches help in simplifying the mining procedure for accomplishing latency improvement and energy savings. Another possible solution for meliorating blockchain's efficacy is through developing off-chain blockchain methods [68] by combining hybrid consensus techniques with cloud services. These methods are competent of alleviating storage and information processing overload on CoT systems and enhancing the scalability problems of BCoT networks.

B. BCoT with Big data

Big data has loomed as a vital data analytic technique for examining the capacity of information discovery from mighty IoT blockchain data. It is anticipated that BCoT may witness a drastic rise in information traffic due to the variety, volume and velocity of blockchain information in the emerging networks. Utilization of big data technology can favor innumerable solutions for provisioning BCoT networks, including data cleaning, analytics and storage [69]. It can even provide cleaning services for enhancing data quality. Furthermore, processing and analysis of information can be enacted through data analytics methods like MapReduce processing and data clustering schemes. Integration of big data with BCoT can aid in improved privacy preservation and data integrity for ensuring secure data analytics in big data. In BCoT, blockchain arises as the prime candidate for fixing big data pertinent problems [70]. Undeniably the blockchain's decentralized feature associated with reliability and authentication can provide strong security to resources of big data. Particularly, blockchain can furnish trustworthiness and transparency for big data distribution among data owners and SPs.

Through eliminating fright of security obstacles, BCoT can entitle universal information exchange thus empowering far-reaching BCoT deployments.

C. Artificial intelligence with BCoT

The future BCoT's prime vision is to offer ubiquitous CoT services with security enhancements and system performance advancements for fulfilling the incrementing needs of emerging services and users in the imminent networks. For realizing these objectives, strategies for crucial BCoT network concerns like resource scheduling, system management and network optimization are extremely necessary. Many existing solutions rely on centralized designs or classical optimization methods, which pose some vital challenges. For instance, massive volumes of IoT data in emerging BCoT platforms can make classical data processing schemes unproductive. Also the huge dynamics of data traffic in IoT can make service and computation management challenging. For surmounting these difficulties, artificial intelligence (AI) methods have appeared as streamlined solutions. These methods serve as favorable candidates for supporting upcoming BCoT applications. In the AI domain, crucial enabling technologies like deep learning, machine learning are applied successfully in several areas, including speech recognition, medical diagnosis, business marketing, share prediction, computer vision and so on. Revolution of AI technology transforms present BCoT services into more advanced ones through improving its potential to learn from acquired data and generate data oriented insights, enable decision support, offer assistance in data classification and prediction for boosting network performances. These technologies help in ameliorating the intelligence of applications [71]. Moreover, they serve as attractive solutions for sorting out several critical problems including security challenges in BCoT systems [72], [73]. Undoubtedly, adoption of AI techniques offers numerous perspectives for analyzing, evaluating and handling existing problems in BCoT environments, thereby allowing to boost performance, security and service quality of the entire network.

D. Mobile cloud

Mobile cloud (MC), an extended wing of CC has loomed as the most innovative and promising technology for empowering BCoT networks. Similar to CC, MC can provide multiple computing services along with competencies of data storage, task processing, QoS improvements and heterogeneity support. Infact, MCs are located within an immediate vicinity of IoT devices, thus enabling remarkably effective IoT information computation along with much less transmission delay than existing remote clouds. Consequently, MC can deliver instant computing services to IoT customers with swift service response and low latency, which might be specifically beneficial in the forthcoming communication systems. The distributed arrangement or configuration of MC also brings several perks, from scalability improvement, pervasive computing services to network complexity diminution for confronting rapidly incrementing IoT service needs and exploding IoT applications [74]. Exploitation of MC technology in BCoT systems can minimize system's energy consumption, network latency and overload on resource-limited IoT gadgets and moreover can boost BCoT network performance.

E. BCoT in future communication networks

The future generation mobile communication networks have reformed the society and industry through delivering an unimaginable range of novelty with certain key benefits like enormous device connectivity, greater system throughput, energy savings, reduced operational expenses, less network latency and elevated data rate. However, the evolution of novel architectures like machine-to-machine (M2M) communications, network function virtualization (NFV), network slicing, CC and software defined networking (SDN) in communication networks has raised multiple security concerns [75]. For instance, SDN networks face certain security impediments like attacks on susceptibilities in switches, faked or forged traffic flows and inadequate trust methods between management and controller applications [76]. Meanwhile, providing the integrity of data between SPs and platforms for avoiding information leakage hazards during resource sharing between servers and NFV users still continues to be an open problem. Under such perspectives, blockchains can offer feasible security countermeasures. Blockchains can construct decentralized authentication approaches for SDN for implementing decentralized access approval with smart agreements [77]. Blockchains can even strengthen trust among existing network entities i.e. network users and SDN controllers through exploiting shared ledgers for secure information exchange and reliable communications. Blockchains in NFV can secure network functions delivery and assure system integrity despite data threats like data attacks and malicious virtual machine tampering [78]. For supporting emerging IoT applications, mobile networks also rely on network slicing. However, its operation also faces inter-slice security problems. For instance, sharing of communication link among multiple slices can provide a chance for malicious users to disrupt data on remaining slices. Through blockchains, reliable network slices can be built. This is accomplished through submitting the request received for establishing a network slice to blockchain for verification or authentication via smart contracts. This can even assist resource providers in executing resource trades on smart agreements. Additionally, data regarding sub-slice deployment can be immutably logged and preserved in blockchain. In M2M communications, blockchains can foster trust between M2M users and assure transparency and authentic information exchange among distinct users. In blockchain-oriented M2M scenario, only edge servers or resourceful devices (like powerful smartphones, laptops) participate in the mining process of blockchain while lightweight devices just participate for communication purposes [79]. Blockchains in mobile communication network operations can support trust management because of its immutable and decentralized features. They can even avoid data threats and identify network attacks through flexible and safe key management. BCoTs can bring ample opportunities to communication network management. The blockchain in BCoT can be utilized for building end-to-end reliable network slices while the cloud-intrinsic architecture with programmable networking can boost communication network's slicing functions with regard to data throughput, network resources and delay. These findings are anticipated to smooth the path for forthcoming BCoT communication networks.

F. Flying IoT devices

The fast advancement of drones or flying IoT devices are creating innumerable fresh business opportunities at commercial level for SPs. These devices are broadly exploited in multifarious realms ranging from healthcare, security, surveillance and military to different monitoring applications. Owing to the swiftly rising IoT traffic in modern communication systems, supporting data requirements of millions of IoT components in widespread BCoT ecosystems has become difficult for stationary base stations (e.g. router, access point). Thus, adoption of drones or mobile IoT devices in these scenarios can handle better data traffic [80]. In fact drones can be utilized as mobile base stations for supporting unaccustomed IoT services like dynamic information offloading, service collaboration or data sharing, because of its flexibility and mobility. Moreover, it is a great choice for coordinating and connecting numerous SPs and IoT users. Recently multiple researches are undertaken on utilization of drones for empowering BCoT applications. The consolidation of blockchain and drones can enable effective content dissemination, facilitate flexible and safe communication, enhance security against data attacks and improve business efficacy.

VII. CONCLUSION

This article presented a deep survey of the integration of CoT and blockchain technologies (BCoT). It provided the motivation, background and scope of BCoT research and discussed the need for integrating CoT and blockchain methods. This paper presented the potential profits of collaborating these key technologies. It reported the vital BCoT applications in distinct use-case domains like smart industry, smart transportation, smart education, intelligent resource management, smart healthcare and intelligent cloud services. It further discussed the significant merits of BCoT. It then discussed the key technical issues and research challenges along with some crucial solutions. This survey finally provided the substantial future directions for undertaking more BCoT research and fostering further innovations in this arena.

REFERENCES

[1] F. Tschorsch, and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Commun. Surv. Tutor., vol. 18, no.3, pp. 2084-2123, 2016.

[2] M. S. Karunarathne et al., “Remote monitoring system enabling cloud technology upon smart phones and inertial sensors for human kinematics,” in 2014 IEEE Fourth International Conference on Big Data and Cloud Computing, IEEE, 2014, December, pp. 137-142.

[3] M. Aazam, et al., “Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved,” in Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014, IEEE, 2014, January, pp. 414-419.

[4] B. Kantarci, and H. T. Mouftah, “Sensing services in cloud-centric Internet of Things: A survey, taxonomy and challenges,” in 2015 IEEE International Conference on Communication Workshop (ICCW) IEEE, 2015, June, pp. 1865-1870.

[5] H. F. Atlam et al., “Integration of cloud computing with internet of things: challenges and open issues,” in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) IEEE, 2017, June, pp. 670-675.

[6] J. Zhou, “Security and privacy for cloud-based IoT: Challenges,” IEEE Commun. Mag., vol. 55, no.1, pp. 26-33, 2017.

[7] M. S. Ali et al., “Applications of blockchains in the Internet of Things: A comprehensive survey,” IEEE Communi. Surv. Tutor., vol. 21, no.2, pp. 1676-1717, 2018.

[8] M. A. Ferrag et al., “Blockchain technologies for the internet of things: Research issues and challenges,” IEEE Internet Things J., vol. 6, no.2, pp. 2188-2204, 2018.

[9] T. M. Fernández-Caramés, and P. Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things,” Ieee Access, vol. 6, pp. 32979-33001, 2018.

[10] 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, 2019.

[11] R. B. Uriarte, and R. DeNicola, “Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards,” IEEE Commun. Stand. Mag., vol. 2, no.3, pp. 22-28, 2018.

[12] M. Wu, et al., “A comprehensive survey of blockchain: From theory to IoT applications and beyond,” IEEE Internet Things J., vol. 6, no.5, pp. 8114-8154, 2019.

[13] R. Yang et al., “Integrated blockchain and edge computing systems: A survey, some research issues and challenges,” IEEE Commun. Surv. Tutor., vol. 21, no.2, pp. 1508-1532, 2019.

[14] J. H. Park, and J. H. Park, “Blockchain security in cloud computing: Use cases, challenges, and solutions,” Symmetry, vol. 9, no.8, p. 164, 2017.

[15] S. Nayak et al., “Saranyu: Using smart contracts and blockchain for cloud tenant management,” in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) IEEE, 2018, July, pp. 857-861.

[16] A. Alammary et al., “Blockchain-based applications in education: A systematic review,” Appl. Sci., vol. 9, no.12, p. 2400, 2019.

[17] M. A. Rahman et al., “Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city,” IEEE Access, vol. 7, pp. 18611-18621, 2019.

[18] H. Yu, Z. Yang, and R. O. Sinnott, “Decentralized big data auditing for smart city environments leveraging blockchain technology,” IEEE Access, vol. 7, pp. 6288-6296, 2018.

[19] S. Singh et al., “SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology,” Int. J. Distrib. Sens. Netw., vol.15, no.4, p. 1550147719844159, 2019.

[20] M. Sookhak et al., “Security and privacy of smart cities: a survey, research issues and challenges,” IEEE Commun. Surv. Tutor., vol. 21, no.2, pp. 1718-1743, 2018.

[21] S. Khezr et al., “Blockchain technology in healthcare: A comprehensive review and directions for future research,” Appl. Sci., vol. 9, no.9, p. 1736, 2019.

[22] M. Hölbl et al., “A systematic review of the use of blockchain in healthcare,” Symmetry, vol. 10, no.10, p.470, 2018.

[23] S. Li, and P. N. Pathirana, “Cloud-based non-invasive tele-rehabilitation exercise monitoring,” in 2014 IEEE Conference on Biomedical Engineering and Sciences (IECBES) IEEE. 2014, December, pp. 385-390.

[24] H. T. Pham, and P. N. Pathirana, “Measurement and assessment of hand functionality via a cloud-based implementation,” in International Conference on Smart Homes and Health Telematics Springer, Cham, 2015, June, pp. 289-294.

[25] A. Al Omar et al., “Privacy-friendly platform for healthcare data in cloud based on blockchain environment,” Future Gener. Comput. Syst., vol. 95, pp. 511-521, 2019.

[26] H. Wang, and Y. Song, “Secure cloud-based EHR system using attribute-based cryptosystem and blockchain,” J. Med. Syst., vol. 42, no.8, pp.1-9, 2018.

[27] D. C. Nguyen, K. D. Nguyen, and P. N. Pathirana, “A mobile cloud based iomt framework for automated health assessment and management,” in 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) IEEE, 2019, July, pp. 6517-6520.

[28] A. D. Dwivedi et al., “A decentralized privacy-preserving healthcare blockchain for IoT,” Sens., vol. 19, no.2, p. 326, 2019.

[29] S. Cao et al., “Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain,” Inf. Sci., vol. 485, pp. 427-440, 2019.

[30] H. Kaur et al., “A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment,” J. Med. Syst. vol. 42, no.8, pp.1-11, 2018.

[31] H. Jin et al., “A review of secure and privacy-preserving medical data sharing,” IEEE Access, vol. 7, pp. 61656-61669, 2019.

[32] J. Liu, et al., “BPDS: A blockchain based privacy-preserving data sharing for electronic medical records,” in 2018 IEEE Global Communications Conference (GLOBECOM) IEEE, 2018, December, pp. 1-6.

[33] X. Liang et al., “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC) IEEE, 2017, October, pp. 1-5.

[34] S. Wang, Y. Zhang, and Y. Zhang, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems,” Ieee Access, vol. 6, pp. 38437-38450, 2018.

[35] X. Zheng et al., “Blockchain-based personal health data sharing system using cloud storage,” in 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) IEEE, 2018, September, pp. 1-6.

[36] Q. I. Xia et al., “MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,” IEEE Access, vol. 5, pp. 14757-14767, 2017.

[37] Q. Xia et al., “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” Inf., vol. 8, no.2, p.44, 2017.

[38] Y. Du et al., “A medical information service platform based on distributed cloud and blockchain,” in 2018 IEEE International Conference on Smart Cloud (SmartCloud) IEEE, 2018, September, pp. 34-39.

[39] R. C. Celiz, Y. E. De La Cruz, and D. M. Sanchez, “Cloud model for purchase management in health sector of peru based on IoT and blockchain,” in 2018 IEEE 9th

Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) IEEE, 2018, November, pp. 328-334.

[40] J. Park et al., “CORUS: Blockchain-based trustworthy evaluation system for efficacy of healthcare remedies,” in 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) IEEE, 2018, December, pp. 181-184.

[41] G. Perboli, S. Musso, and M. Rosano, “Blockchain in logistics and supply chain: A lean approach for designing real-world use cases,” Ieee Access, vol. 6, pp.62018-62028, 2018.

[42] D. E. O'Leary, “Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems,” Intell. Syst. Account, Financ. Manag., vol. 24, no.4, pp.138-147, 2017.

[43] N. Mohamed, J. Al-Jaroodi, and S. Lazarova-Molnar, “Leveraging the capabilities of industry 4.0 for improving energy efficiency in smart factories,” Ieee Access, vol. 7, pp. 18008-18020, 2019.

[44] A. Bahga, and V. K. Madisetti, “Blockchain platform for industrial internet of things,” J. Softw. Eng. Appl., vol.9, no.10, pp.533-546, 2016.

[45] T. Yang et al., “Applying blockchain technology to decentralized operation in future energy internet,” in 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2) IEEE, 2017, November, pp. 1-5.

[46] S. Wang et al., “Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids,” IEEE Trans. Syst. Man Cybern. Syst., vol.49, no.8, pp.1612-1623, 2019.

[47] S. Nadeem et al., “Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture,” Int. J. Adv. Comput. Sci. Appl., vol.10, no.1, pp. 288-295, 2019.

[48] X. Zhang, R. Li, and B. Cui, “A security architecture of VANET based on blockchain and mobile edge computing,” in 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) IEEE, 2018, August, pp. 258-259.

[49] A. Dorri et al., “Blockchain: A distributed solution to automotive security and privacy,” IEEE Commun. Mag., vol.55, no.12, pp.119-125, 2017.

[50] M. Li, L. Zhu, and X. Lin, “Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing,” IEEE Internet Things J., vol. 6, no.3, pp.4573-4584, 2018.

[51] J. Fan, R. Li, and S. Li, “Research on task scheduling strategy: Based on smart contract in vehicular cloud computing environment,” in 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) IEEE, 2018, August, pp. 248-249.

[52] Z. Li et al., “Blockchain and IoT data analytics for fine-grained transportation insurance,” in 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS) IEEE, 2018, December, pp. 1022-1027.

[53] L. Xie et al., “Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs,” IEEE Access, vol. 7, pp. 56656-56666, 2019.

[54] B. Yin et al., "Joint cloud collaboration mechanism between vehicle clouds based on blockchain," in 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE) IEEE, 2019, April, pp. 227-2275.

[55] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," IEEE Netw., vol. 32, no.3, pp. 78-83, 2018.

[56] Y. Zhang et al., "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," Inf. Sci., vol. 462, pp. 262-277, 2018.

[57] J. Zhou et al., "Security and privacy for cloud-based IoT: Challenges," IEEE Commun. Mag., vol. 55, no.1, pp.26-33, 2017.

[58] M. A. Khan, "A survey of security issues for cloud computing," J. Netw. Comput. Appl., vol. 71, pp.11-29, 2016.

[59] X. Li et al., "A survey on the security of blockchain systems," Future Gener. Comput. Syst., vol.107, pp. 841-853, 2020.

[60] S. Rouhani, and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," IEEE Access, vol. 7, pp. 50759-50779, 2019.

[61] M. Wohrer, and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," in 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE) IEEE, 2018, March, pp. 2-8.

[62] A. Anjum, M. Sporny, and A. Sill, "Blockchain standards for compliance and trust," IEEE Cloud Comput., vol.4, no.4, pp. 84-90, 2017.

[63] X. Li et al., "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach," IEEE Access, vol. 7, pp. 9368-9383, 2019.

[64] R. Cheng et al., "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts," in 2019 IEEE European Symposium on Security and Privacy (EuroS&P) IEEE, 2019, June, pp. 185-200.

[65] C., Stergiou et al., "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," Sustain. Comput.: Inform. Syst., vol.19, pp.174-184, 2018.

[66] Y. Liu et al., "$\mathsf {LightChain} $: A Lightweight Blockchain System for Industrial Internet of Things," IEEE Trans. Ind. Inform., vol.15, no.6, pp.3571-3581, 2019.

[67] T. Kim, J. Noh, and S. Cho, "SCC: storage compression consensus for blockchain in lightweight IoT network," in 2019 IEEE International Conference on Consumer Electronics (ICCE) IEEE, 2019, January, pp. 1-4.

[68] Y. Tang et al., "ChainFS: Blockchain-secured cloud storage," in 2018 IEEE 11th international conference on cloud computing (CLOUD) IEEE, 2018, July, pp. 987-990.

[69] M. Ge, H. Bangui, and B. Buhnova, "Big data for internet of things: a survey," Future Gener. Comput. Syst., vol. 87, pp. 601-614, 2018.

[70] E. Karafiloski, and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in IEEE EUROCON 2017-17th International Conference on Smart Technologies IEEE, 2017, July, pp. 763-768.

[71] Z. Khan, A. Anjum, and S. L. Kiani, “Cloud based big data analytics for smart future cities,” in 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing, IEEE, 2013, December, pp. 381-386.

[72] D. C. Nguyen et al., “Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning,” IEEE Trans. Netw. Serv. Manag., vol. 17, no.4, pp.2536-2549, 2020.

[73] D. C. Nguyen et al., “Secure computation offloading in blockchain based IoT networks with deep reinforcement learning,” 2019. arXiv preprint arXiv:1908.07466.

[74] H. C. Hsieh, C. S. Lee, and J. L. Chen, “Mobile edge computing platform with container-based virtualization technology for IoT applications,” Wirel. Pers. Commun., vol.102, no.1, pp.527-542, 2018.

[75] D. Fang, Y. Qian, and R. Q. Hu, “Security for 5G mobile wireless networks,” IEEE Access, vol.6, pp. 4850-4874, 2017.

[76] D. Fang, and Y. Qian, “5G wireless security and privacy: Architecture and flexible mechanisms,” IEEE Veh. Technol. Mag., vol.15, no.2, pp. 58-64, 2020.

[77] G. S. Aujla et al., “Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications,” IEEE Netw., vol. 34, no.2, pp.83-91, 2020.

[78] R. V. Rosa, and C. E. Rothenberg, “Blockchain-based decentralized applications for multiple administrative domain networking,” IEEE Commun. Stand. Mag., vol. 2, no.3, pp. 29-37, 2018.

[79] H. Cui et al., “Blockchain-driven contents sharing strategy for wireless cache-enabled D2D networks,” in 2019 IEEE International Conference on Communications Workshops (ICC Workshops) IEEE, 2019, May, pp. 1-5.

[80] N. Nomikos et al., “A UAV-based moving 5G RAN for massive connectivity of mobile users and IoT devices,” Veh. Commun., vol. 25, p. 100250, 2020.