Journal of Network and Computer Applications 226 (2024) 103884

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review article

Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications

Tri Nguyen [a,*,1], Huong Nguyen [a,1], Tuan Nguyen Gia [b,1]

[a] Center for Ubiquitous Computing, University of Oulu, Finland
[b] Silo AI, Finland

ARTICLE INFO

Keywords:
Edge computing
Blockchain
Internet-of-thing
Architecture
Security
Application

ABSTRACT

IoT systems are widely used in various applications, including healthcare, agriculture, manufacturing, and smart cities. However, these systems still have limitations, such as lack of security, high latency, energy inefficiency, the inefficiency of bandwidth utilization, and shortage of automaticity. The integration of edge computing and blockchain into IoT has been proposed to address these limitations. Yet, this integration is challenging and has not been deeply investigated. This paper aims to conduct a review of the integration of edge computing and blockchain into IoT systems. To the best of our knowledge, this is the first review paper that covers all aspects of system architectures and categories of blockchain-based edge deployment, complete security requirements, including confidentiality, integrity, authentication, authorization/access control, privacy, trust/confidence, transparency, availability, secure automaticity, and tolerance, and applications of blockchain-based edge potential usages with consideration of security requirements. Additionally, this review provides comprehensive discussions of challenges and insights into the future direction of blockchain-based edge IoT systems. The review aims to serve as an entry point for non-expert readers and researchers to various aspects of blockchain-based edge IoT systems.

1. Introduction

Internet-of-Things (IoT) (Sundmaeker et al., 2010; Moosavi et al., 2015; Gia et al., 2014) is a paradigm of integrating objects to cyber and physical world that enable sensing, identifying, networking, computation, and control. For example, an IoT-based healthcare system can consist of wearable sensors that collect bio-signals from patients and transmit the collected data over a wireless network to cloud servers. A medical doctor can use a mobile application or an Internet browser to access the e-health data captured from many patients simultaneously. As a result, work efficiency increases, and the shortage of medical personnel can be partly overcome (Gia et al., 2015). However, IoT still has many disadvantages, such as lack of security, unreliability, energy inefficiency, and centralized data storage (Fetahu et al., 2022; Talebkhah et al., 2021). For instance, when the Internet connection between IoT devices and cloud servers is interrupted, IoT services cannot be maintained properly.

Edge computing, which can be described as a distributed computing paradigm enabling computation and storage closer to the source of data, can solve the above-mentioned IoT limitations. Instead of transmitting all the collected data to cloud servers for further processing, some parts of the data can be stored and processed at edge devices (e.g., edge computer or edge gateway). This enables real-time analysis and decision-making that might require Artificial Intelligence (AI) (Queralta et al., 2019; Gia et al., 2019). For instance, resource-constrained edge devices (e.g., drones, Unmanned Aerial Vehicles (UAVs), or edge computers) can detect persons in real-time from a live video by running YOLO4, YOLO5, and YOLOX algorithms which are single-stage object detectors based on DarkNet53 convolution networks (Nguyen et al., 2021b, 2023a). In addition, edge computing enhances some security levels of IoT systems by running cryptography primitives or algorithms at the edge devices. This helps protect data transmitted over a network. Nonetheless, applying edge computing cannot completely solve all the issues of IoT systems (Xiao et al., 2019). For instance, edge-based IoT systems still rely on centralized cloud servers, which can lead to security risks and a single point of failure.

Fortunately, the drawback of centralized cloud servers in edge-based IoT systems can be tackled by blockchain which is a digital ledger of transactions featuring decentralization, transparency, automatic processes, increased trust, and reduced fraud. However, it is challenging to

* Corresponding author.
E-mail addresses: tri.nguyen@oulu.fi (T. Nguyen), huong.nguyen@oulu.fi (H. Nguyen), tunggi@utu.fi (T. Nguyen Gia).
[1] Authors contributed equally.

https://doi.org/10.1016/j.jnca.2024.103884
Received 1 September 2023; Received in revised form 8 March 2024; Accepted 13 April 2024
Available online 22 April 2024

Table 1
Acronyms.

Abbr.	Definition
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AVR	Alf-Egil Bogen Vegard Wollan RISC
BLE	Bluetooth Low Energy
CNN	Convolution Neural Network
CPU	Central Processing Unit
DoS	Denial of Service
ECC	Elliptic-curve Cryptography
ECG	Electrocardiogram
EEG	Electroencephalogram
EMG	Electromyography
Edge-AI	Artificial Intelligence at the Edge
EoT	Edge of Things
EI	Edge Intelligence
EOG	Electrooculogram
FDA	United States Food and Drug Administration
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
IoT	Internet-of-Things
LoRa	Long range
MEC	Mobile Edge Computing
MCC	Mobile Cloud Computing
PaaS	Platform as a Service
P2P	Peer-to-peer
RNN	Recurrent neural network
SaaS	Software as a Service
SaR	Search and Rescue
UAVs	Unmanned Aerial Vehicles

efficiently apply blockchain in edge-based IoT systems because edge devices often have limited processing power, memory, and storage capacity, whilst blockchain requires heavy computation. This paper aims to investigate approaches that overcome the challenges. Particularly, this paper discusses several advanced system architectures that efficiently utilize state-of-the-art technologies, including edge computing, AI at the edge, IoT, and blockchain. Based on the architectures, the security requirements are discussed together with recommended solutions. The main contributions of this article are as follows:

- Introducing system architecture of the smart blockchain-based edge IoT system
- Investigating different implementations of blockchain on IoT systems
- Deep analyzing security requirements and suggesting solutions for fulfilling these requirements
- Representing different applications, including smart healthcare, smart grid, and maritime Search and Rescue (SaR) using blockchain-based edge IoT systems

The structure of the paper is as follows: The literature review of similar works is in Section 7. Section 2 discusses preliminaries of distributed computing models with the edge, fog, and cloud perspectives, while a brief mention of blockchain technology is in Section 3. Then, Section 4 is potential couplings of blockchain and distributed computing models, especially those interested in edge computing. Section 5 mentions security requirements, while the applications of blockchain-based edge IoT systems are presented in Section 6. Section 7 discusses motivations and state-of-the-art reviews focusing on edge/fog IoT, blockchain IoT, and edge blockchain. Section 8 points discussions from our viewpoints, while research directions to explore new opportunities and advancements are presented in Section 9. Finally, Section 10 concludes this work. To be convenient for readers, abbreviations used in this article are listed in Table 1.

2. Preliminaries: Edge computing, fog computing and cloud computing

In terms of time-critical IoT applications, centralized cloud servers, which are used for data processing, might not be appropriate due to the late response caused by transmissions of large data volumes. Instead, some parts of the data can be stored and processed in a distributed manner at edge and fog devices, that can be considered as edge and fog computing. Particularly, edge computing (Shi et al., 2016; Satyanarayanan, 2017) and fog computing (Bonomi et al., 2012) aim to shift computing from centralized cloud servers to distributed resources closer to where data is captured (Peltonen et al., 2022). Edge and fog computing share many similarities; for instance, they enable an intermediate layer between the data source and cloud servers. The layer proffers capabilities of geographical location awareness and distributed storage and computation. However, these computing paradigms are not identical. Detail of these computing types are presented as follows:

2.1. Edge computing

As depicted in Fig. 1, edge computing is the closest layer to the source where data is generated (Metwaly et al., 2019). Edge computing can consist of different edge devices such as wearable devices, resource-constrained devices, or edge gateways (e.g., Raspberry Pi or Pandaboard-based edge gateways (Gia et al., 2014)). Edge computing enables various edge services, including real-time analytics, distributed storage, location awareness, interoperability support, mobility support, and edge-AI, which help enhance the quality of service significantly (Nawaz et al., 2020; Metwaly et al., 2019; Nguyen Gia et al., 2020). For instance, medical data captured by wearable devices can be stored in a distributed manner in a local gateway or a network of edge gateways. When a medical doctor wants to access the captured data, it will be retrieved directly from these edge devices. This significantly reduces transmission latency. Edge computing also enhances security levels and energy efficiency by encrypting data transmitted over a network and offloading heavy computational tasks to more powerful devices, respectively.

In regard to edge-AI, complex AI models are often trained at cloud servers, and the final models are then deployed at edge devices to provide instant results and support real-time decision-making. For example, Long Short-Term Memory Neural Network (LSTM) models can be run at edge for detecting cardiovascular diseases by analyzing time-series electrocardiogram (ECG) data. However, due to limited resources, not all tasks can be carried out efficiently at edge layer. Particularly, only tasks that do not require intensive computation and large memory storage are run at edge devices.

Edge computing can be categorized based on architectural paradigms, deployment models, or particular usage. Multi-access Edge Computing (MEC), which has been standardized by The European Telecommunications Standards Institute, is an edge computing type, specifically designed to work with cellular networks (Hu et al., 2015; Mao et al., 2017; Abbas et al., 2017). MEC deploys and leverages distributed base stations for edge computing. Another edge computing type is cloudlets which consist of micro data centers positioned at the edge of a network (Satyanarayanan et al., 2009). Dissimilar to MEC, cloudlets can be used for various scenarios including wired and wireless networks (Dolui and Datta, 2017). Another type is industrial edge computing which consists of edge devices which are specified for fulfilling industrial standards and requirements such as robustness, reliability, scalability, temperature tolerance, security, and industrial communication protocol support.

2.2. Fog computing

Fog computing, as depicted in Fig. 1, was first introduced by Cisco in 2012 as a mid-layer computing paradigm that brings cloud computing

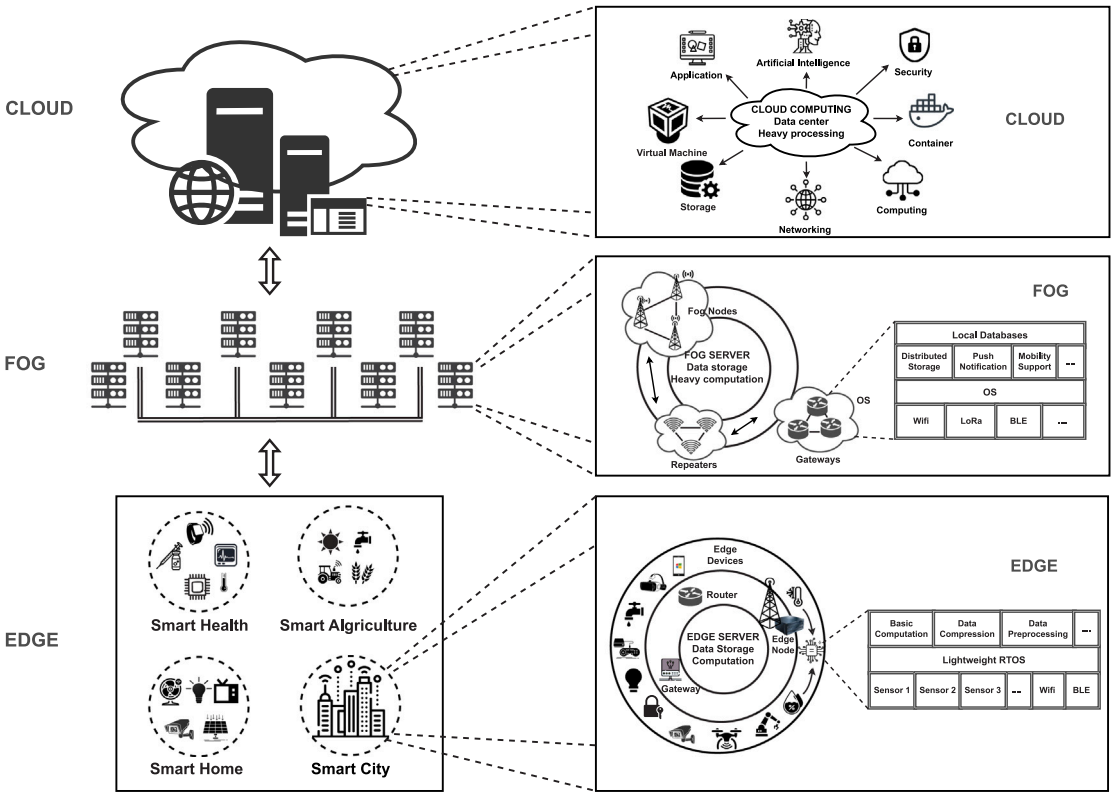

Fig. 1. Edge-Fog-Cloud: a general and closer look.

capabilities closer to the edge of the network (Mahmud et al., 2018; Gia et al., 2015). Fog computing can be considered as the middle layer between edge computing and cloud computing. It encompasses not only computation capabilities but also networking, storage, and other services. The networking components in fog computing address geographical coverage and high latency issues by managing network resources and supporting mobility as well as location awareness of multiple distributed fog nodes over areas. To provide these services, fog computing estimates or tracks the physical locations of connected devices and the possibility of these devices moving out of coverage range or from one coverage area into another. Components such as routers, access points, switches, or base stations can make up the fog layer (Yi et al., 2015). Depending on the application, the number of fog devices can vary, and the network topology of these devices may differ, such as in a star or mesh network. Additionally, the fog layer includes servers that store temporary data, which can be purged after a while (e.g. every few weeks). Compared to edge computing, fog often consists of more powerful network-related devices and servers than those used at edge. Therefore, the fog layer can perform more advanced analytic and dynamic resource allocation. Fog computing often covers larger area networks, such as networks of several buildings having dozens or hundreds of devices, whilst edge computing often refers to smaller networks, such as across several wearable devices or IoT devices in a smart home. Accordingly, the amount of data in fog is often much larger than the data aggregating at edge devices. Fog computing is especially important in situations where a large amount of data is transmitted over the network, and many resources are needed to maintain communication quality (Yi et al., 2015). Although fog devices are powerful, not all tasks can be processed in the fog, such as heavy computational tasks for training deep learning-based models with dozens or even hundreds of layers. Thus, it is crucial to determine which tasks should be carried out in the fog and which should be processed in further layers, such as cloud servers, to achieve high energy efficiency and low latency.

2.3. Cloud computing

In Fig. 1, the cloud is presented as the farthest layer that offers many advanced services, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), serverless, and Software-as-a-Service (SaaS). Cloud computing provides robust capacity, global storage, and scalability, making it an ideal paradigm for many applications. One of the main benefits of cloud computing is its ability to back up data on different offsite storage locations, ensuring data recovery after hardware or software failures. Cloud computing also provides easy access to data from any location or device. Additionally, cloud services can be elastically scaled up or down to meet changing computing, storage, or network bandwidth demands. However, this highest layer still has many drawbacks, such as security risks, high latency, and a single point of failure. Cloud servers are usually centralized in one location, geographically far from IoT devices. As a result, sending or requesting data can take a large latency. When there are thousands or even millions of geo-distributed devices in the network, this latency problem worsens. Furthermore, long-distance transfer also affects data confidentiality, increasing the risk of data loss or leakage. Fortunately, some of the issues can be addressed by edge and fog computing.

Table 2 summarizes various types of computing such as edge, fog, and cloud computing. While cloud computing stands apart from the rest, other computing types have many similarities, such as distributed data storage and computation, mobility support and location awareness. These computing paradigms help enhance the quality of service by conserving network bandwidth, reducing latency, and providing fault tolerance (Pan et al., 2018).

3. Blockchain technology

3.1. Blockchain technology

Blockchain technology fosters trust among participants by utilizing a unique database (Nakamoto, 2008). Blockchain owes its success to

Table 2
Features comparison among different types of Edge, Fog, and Cloud computing.

Paradigms	MEC (Hu et al., 2015; Mao et al., 2017; Abbas et al., 2017)	Cloudlet (Satyanarayanan et al., 2009)	Edge (Shi et al., 2016; Satyanarayanan, 2017)	Fog (Bonomi et al., 2012)	Cloud (Jadeja and Modi, 2012; Armbrust et al., 2010),
Users	Mobile	Mobile	General/Mobile	General	General
Distribution	Distributed	Distributed	Distributed	Distributed	Centralized
Distance to data	Close	Close	Close	Relatively close	Far
Storage capacity	Low	Low	Low	Low	High
Data keeping	Transient	Transient	Transient	Transient	Permanent
Service	Local	Local	Local	Local	Global
Internet connection	Little/Not needed	Little/Not needed	Little/Not needed	Little/Not needed	Needed
Communication latency	Low	Low	Low	Low	High
Mobility	Supported	Supported	Supported	Supported	Limited (MCC only)
Large-scaled application	Supported	Not supported	Supported	Supported	Supported
Visualization	Supported	Supported	Not supported	Supported	Supported
Real-time application	Supported	Supported	Supported	Supported	Not supported
Location awareness	Supported	Supported	Supported	Supported	Not supported

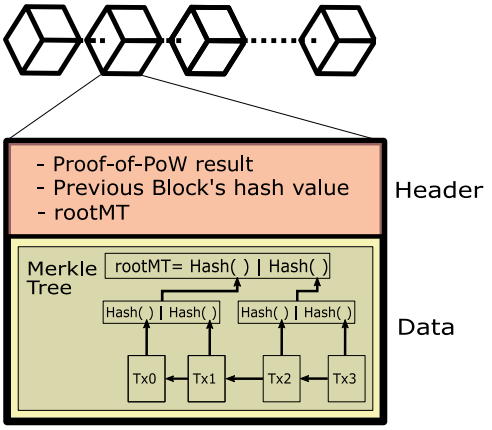

Fig. 2. Blockchain structure: The header includes metadata, and data is a set of transactions. In detail, the Proof-of-Work result is about the evidence to form this block, and rootMT is the final value from the Merkle root tree calculated from the data side.

the immutability of confirmed data among all participants via a hash pointer scheme. In other words, blockchain enables participants to maintain and observe a consistent view of the entire system, thereby promoting trust. As shown in Fig. 2, blockchain consists of a chain of blocks in which each block comprises the header section and the data section. The header contains metadata such as timestamps, connections to previously confirmed blocks, consensus proof, and checksum of stored data using Merkle tree structure (Merkle, 1987) and hashing functions. The data section is used to store a series of interconnected transactions in the form of messages.

Generally, blockchain technology is composed of several essential components, such as consensus, access, cryptographic schemes, workflow, and data model (Belotti et al., 2019). The consensus component aims to reach an agreement among participants before creating block candidates, while cryptographic schemes address privacy and security concerns, particularly in communication. The workflow component governs the system procedures for handling requests. For example, most blockchain platforms operate on an order-execution basis, which requires agreement on the transaction order before execution. The data model is responsible for organizing data within the system. Although various types of models exist, such as unspent transaction output, account-based, or key–value models, account-based is the most widely used in blockchain platforms.

Blockchain is a critical technology that enables decentralized solutions, but it can also result in unintended consequences (Nguyen et al., 2021c). Decentralization requires identical participants to reach a consensus mechanism for updates, which differs from centralization where decisions are made from a focal point. Thus, the use of blockchain requires greater attention to performance since the consensus process demands significant communication efforts among participants to elect a leader or achieve unique agreements.

3.2. Blockchain categories and platforms

Blockchain types are often categorized based on their access perspective, as described in several studies (Wang et al., 2019; Belotti et al., 2019; Nguyen et al., 2021c). Permissioned blockchain refers to a blockchain system that restricts network access to identified participants. These participants are granted permission to contribute to and maintain the blockchain system. On the other hand, permissionless blockchain allows participants to join and leave freely, with no restrictions on data access. However, becoming notable in a permissionless blockchain requires a significant contribution to the system's development. In contrast, consortium blockchain provides identities to participants, but the system's data is publicly accessible. Unlike permissioned and permissionless blockchains, consortium blockchains enable controlled and regulated data access.

Due to the variety of categories, blockchain platforms have become diverse in different aspects. Although current research primarily focuses on simulations, the practical deployment of blockchain platforms in edge computing and IoT is based on two representatives, Hyperledger Fabric (Androulaki et al., 2018) and Ethereum (Wood et al., 2014; Buterin, 2014). Hyperledger is a representative of a permissioned blockchain, while Ethereum is one of the permissionless blockchains. Due to the permission requirements, participants in Hyperledger Fabric must provide an identity to join the system, whereas participants in Ethereum do not require a real identity. From the viewpoint of accessibility, the performance and procedures of these platforms differ. For instance, with the real identity of participants in Hyperledger Fabric, the consensus and propagation processes are more efficient than in Ethereum. However, using identity can affect participants' privacy and reduce the level of decentralization in systems (Nguyen et al., 2023b).

3.3. Blockchain development

With blockchain benefits, many research have been exploiting the usage of blockchain in various aspects, for example, blockchain-based smart contracts for decentralized applications and blockchain-as-a-service with token management. Also, off-chain is a solution for applications that distribute large data.

3.3.1. Smart contract

The emergence of blockchain-based smart contracts marks the next generation of blockchain technology. Ethereum is a notable contributor in this regard, leveraging Turing-complete machines to create a set of operations known as smart contracts. Essentially, smart contracts are programmable sequences of execution that are distributed to a range of participants. This enables autonomous execution among participants, facilitating decentralized applications, and decentralized autonomous organizations that operate with automation and self-organization (Buterin, 2014).

3.3.2. Off-chain

Blockchain can experience communication and storage overload due to the storage requirements for network participants. To address this limitation, the InterPlanetary File System (IPFS) (Chen et al., 2017; Zheng et al., 2018) suggests that IPFS can be used to store data based on the blockchain while the blockchain maintains the hash of transactions. As a result, a significant amount of data in the blockchain can be moved to IPFS for storage, which reduces the resource requirements of the blockchain.

3.3.3. Blockchain-as-a-service

Blockchain-as-a-Service refers to utilizing blockchain technology in supporting services such as token management, reputation management, and incentive strategies. Since blockchain technology has proven successful in cryptocurrency, it has been primarily associated with incentive strategies for rewarding compliant participants and punishing those who are not. As a result, blockchain has been used to manage the reward system for system contributors and punish wrongdoers, especially in resource trading studies (Han et al., 2022). An interesting consideration for BaaS is blockchain-based reputation management (Schaub et al., 2016; Sharples and Domingue, 2016; Hasan et al., 2022). Blockchain provides a service that maintains reputation scores, indicating the level of trust among participants based on the history of feedback. This allows for a more transparent and reliable reputation management system.

4. Blockchain-based edge IoT architecture

This section provides an overview of the system architectures utilizing blockchain, edge computing, edge-AI, and IoT. In addition, it examines the practical locations where blockchain can be deployed, including edge devices and cloud servers.

4.1. System blockchain-based edge IoT system architecture

As shown in Fig. 3, the system architecture utilizing blockchain, edge-AI, and IoT contains six parts, including the sensor layer, edge layer, networking layer, blockchain layer, third parties, and cloud with terminal applications.

4.1.1. Sensor layer

The sensor layer comprises various resource-constrained sensing devices which can be mobile or fixed in specific locations as Fig. 3. Each device consists of four main components such as a microcontroller, sensors, a wireless/wired communication module, and a power source. Depending on the application, some devices may include additional components such as actuators. The microcontroller used in these devices is typically energy-efficient but has limited computation and memory capacity. For example, an 8-bit AVR microcontroller and a 32-bit 48MHz ARM Cortex-M0 microcontroller are often used in sensing devices. Diving deeper into the heart of sensing technology, the choice between a 32-bit ARM Cortex and an 8-bit AVR microcontroller becomes a strategic decision balancing power and efficiency. The 32-bit ARM Cortex, with its superior processing capabilities, expansive

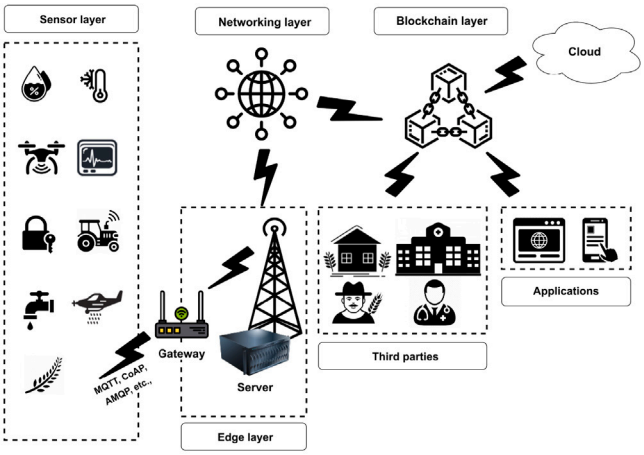

Fig. 3. A general architecture for the integration between blockchain and computing systems.

flash, and RAM memories, is the heavyweight champion for applications demanding high computation and robust security measures. On the other hand, the lightweight contender, the 8-bit AVR, shines in scenarios prioritizing low power consumption and simplicity, perfectly suited for basic tasks like data acquisition and low-frequency data transmission. The ARM Cortex's prowess is further augmented by its support for Memory Protection Units (MPUs), enabling precise memory access control across various regions to shield sensitive code and data from prying eyes. Moreover, the integration of hardware-based security features, including advanced encryption, fortifies the device's defenses, ensuring a bastion of security at the edge of the network. These microcontrollers also master the art of energy conservation, with sleep modes that whisper to the promise of long operational lifetimes, waking only to perform their crucial duties before slipping back into slumber. Directly tethered to these microcontrollers, sensors—be they analog or digital—serve as the frontline scouts of the IoT realm, vigilantly gathering data from the environment. This data, potentially a mix of raw and encrypted information, embarks on its journey to the microcontroller via General Purpose Input-Output (GPIO) ports, ready to be processed or sent forth to the next echelon of the system's architecture. At this juncture, the narrative of data security takes a pivotal turn. The application of cryptography—whether through the simplicity and efficiency of symmetric-key algorithms like AES and DES, or the robust security offered by asymmetric-key counterparts such as RSA, DSA, and ECC—becomes a critical maneuver in the defense against data breaches and unauthorized access. Executed through either software or the more efficient hardware approach, these cryptographic measures, despite their energy and latency trade-offs, stand as guardians of data integrity, especially in applications where security cannot be compromised. Selecting the appropriate cryptographic algorithm thus emerges as a crucial strategy, balancing the scales of security needs against the constraints of energy consumption and processing time. Therefore, the orchestration of microcontrollers, sensors, and cryptographic protocols plays a pivotal role in sculpting the security landscape of IoT systems, weaving a tapestry of technology that safeguards data from sensor to cloud.

Depending on the application, specific wireless communication protocols (e.g. Wi-Fi, BLE5, 6LoWPAN, Zigbee, or LoRa) will be used. For instance, Wi-Fi is commonly used for high data rate applications but consumes large amounts of power whilst BLE5 is more energy-efficient but cannot be used for high data rates exceeding 2Mbps. Beyond the foregoing, mobile devices are usually powered by a Lithium battery, which often has a limited capacity, such as less than 1000mAh for wearable devices. In this delicate ballet of technology, the selection of microcontrollers, sensors, and wireless communication protocols must

be orchestrated with precision. Each component, a soloist in its own right, needs to perform in perfect harmony with the others to optimize the device's operational longevity and meet the stringent demands of the system. This symphony of choices is pivotal, not only for ensuring the seamless functionality of sensing devices but also for navigating the constraints imposed by their limited resources. Among these considerations is the reality that such devices, resource-constrained as they are, find themselves on the sidelines of the blockchain arena, unable to serve as nodes within this distributed ledger's complex choreography.

4.1.2. Edge layer

The edge layer can include edge gateways and edge servers in which gateways mainly receive the data from sensing devices and send it to upper layers shown in Fig. 3. In which, gateways are often fixed in particular locations and supplied from wall power sockets and have more power than sensing devices. For instance, edge gateways can be built with edge hardware such as Raspberry PI and Nvidia Jetson that have 4–6 (1.2–1.5 GHz) ARM cores and 4–8 GB RAM. Therefore, gateways can run more complex algorithms than edge-sensing devices. It can run wavelet transformation algorithms to extract heartbeats from ECG data in real-time and cryptography algorithms to protect data transmitted over a network with a minimal effect on the total latency. In Nguyen Gia et al. (2017), the authors show that applying AES-256 at a gateway built from a low-cost Orange Pi One having 600MHz H3 Quad-core Cortex-A7 increases only 42 μs which is extremely small compared with the total latency. Empowered by their robust capabilities, edge devices transcend their conventional roles to serve as pivotal nodes within the blockchain's intricate network, adeptly meeting and exceeding system requirements. These technological powerhouses are fortified with specialized hardware and software, meticulously engineered to master the art of cryptography — encrypting and decrypting data with unwavering precision. Beyond their cryptographic prowess, edge gateways are the guardians of the network's gateway, equipped with an arsenal of defensive software solutions — from firewalls and access control lists to IP blacklisting, traffic filtering, and blocking mechanisms. These digital sentinels stand vigilant, ensuring the sanctity of the network by thwarting unauthorized access and safeguarding against cyber threats.

The vigilance of edge gateways extends into the realm of anomaly detection, where advanced monitoring systems tirelessly scan for signs of irregular behavior or network activity, serving as an early warning system against potential disruptions or security breaches. This multi-layered approach to network security and operational efficiency positions edge devices as critical components in the architecture, seamlessly integrating with blockchain technology to foster a secure, resilient, and high-performing system.

Comparing to edge gateways, edge servers are much more powerful than edge gateways. For example, edge servers can be equipped with CPUs having 8, 16, or more cores, 16 GB or higher GBs of memory, and several hundred GBs of local storage.[2] Edge servers can run complex algorithms and train deep learning AI models e.g., for real-time decision making or analysis. Edge servers are connected with edge gateways via wire (e.g., Gigabit Ethernet) or wireless communication protocols like Wi-Fi. Data received from edge gateways can be temporarily stored in edge servers. When the storage is full, the new data will replace the oldest data. However, it is not compulsory to include separate edge servers. In some applications, an edge device have two roles of both gateway and server. In essence, the symbiotic relationship between edge gateways and edge servers forms the backbone of this cutting-edge ecosystem. These pivotal devices are not just technological marvels but are the very guardians of the quality of service and security bastions within the network. Their advanced computational capabilities and storage solutions ensure that the network does not just function, but thrives under the pressures of real-time data processing and complex decision-making algorithms.

[2] https://www.ibm.com/cloud/blog/architecting-at-the-edge

4.1.3. Networking layer

The networking layer often comprises routers, gateways, repeaters, and base stations. These devices are responsible for maintaining the quality of communication services. At this strategic juncture, the networking layer emerges as the crucial conduit for data flow, bridging the gap between the edge's intelligence and the broader digital world beyond. Its mission is clear: to ensure that every byte of data finds its path efficiently, securely, and reliably. To accomplish this, the layer deploys an arsenal of sophisticated mechanisms designed to streamline the digital traffic flow. Bandwidth management becomes an art form here, with monitoring and traffic shaping techniques skillfully applied to spotlight bandwidth-hungry devices and give precedence to essential traffic, ensuring that vital data never finds itself caught in a digital bottleneck. But the challenges do not stop at the bandwidth. Network congestion looms as a constant threat, skillfully countered by an array of strategies from buffer management to packet scheduling, all meticulously balanced to keep data flowing smoothly. Meanwhile, interference management tactics, including channel selection and signal strength optimization, are deployed like chess moves in a game where connectivity is king.

Enter fog computing (Mahmud et al., 2018), the network's secret weapon against the perils of resource contention and congestion. This layer does not just react; it anticipates, dynamically adjusting resources in a ballet of bytes and bandwidth. Fog computing does not stop at mere traffic management; it infuses the network with intelligence, leveraging deep learning and adaptive algorithms to dissect network traffic, discern behavior patterns, and sniff out abnormalities. This is where technology transcends its own limitations, offering not just a solution, but a visionary approach to preempting security threats, ensuring that the network remains a step ahead, secure and steadfast in its mission to deliver unmatched quality of service.

4.1.4. Blockchain layer

The blockchain layer, with its cryptographic chains of blocks, stands as a testament to the power of decentralization, offering a future where transparency, security, and P2P exchanges reign supreme. Far beyond the capabilities of traditional networks, this layer introduces an era of immutability, auditability, and a trustless environment, empowering users with unparalleled control and assurance in their transactions. Here, in the realm of blockchain, we witness the convergence of technology and trust, a fusion offering boundless possibilities across various applications, from safeguarding health data through private networks to enabling transparent energy trading on public platforms. Hence, as Fig. 3, blockchain technology plays the key role in managing connectivity among the networking layer, third parties, and cloud with terminated applications. Section 3 and Section 8 provide a more detailed discussion of the blockchain network. Depending on the application, a private blockchain network (e.g., Hyperledger Fabric) or a public blockchain network (e.g., Ethereum) can be used. For instance, in health monitoring applications, a private blockchain network may be preferred as only authorized participants can access the private health data of a patient. On the other hand, smart grid applications may refer to a public blockchain network like Ethereum for energy trading because it is unnecessary to identify the energy seller or buyers.

4.1.5. Third parties

In the presented system architecture, third parties refer to participants who join the blockchain network, including organizations (e.g., hospitals, public authorities, manufacturers) and individuals. These parties typically interact with the blockchain network through smart contracts, which are self-executing contracts that automatically enforce the terms and conditions of the agreement between the parties involved. Using smart contracts on the blockchain network can help reduce the need for intermediaries, minimize transaction costs, and increase the efficiency and transparency of the system.

4.1.6. Cloud with terminal applications

Cloud servers are optional in the discussed system architecture shown in Fig. 3. They can be excluded in applications that do not require heavy computational tasks or have strict time requirements. In these cases, data can be stored in blockchain blocks. However, cloud servers are needed in applications requiring real-time monitoring with strict time requirements, such as a few milliseconds or microseconds. There are two types of connections between cloud servers and the system. The first type is a direct connection between cloud servers and the networking layer without going through the blockchain network. The second type is a connection between cloud servers and the network layer, with the blockchain network in between. In either case, data can be directly sent from the edge layer to the cloud server without going through the blockchain network. To avoid the disadvantages of centralized data storage, cloud server data can be purged quickly after a short period, such as a few minutes. In addition, cloud services, such as IaaS, PaaS, SaaS, or Disaster-Recovery-as-a-Service, can be utilized depending on the application. Meanwhile, data can be added to blockchain blocks for decentralized data storage.

The final component in the architecture shown in Fig. 3 is the application layer, which includes mobile applications and terminals such as internet browsers. These applications allow end-users to connect to cloud servers or the blockchain network and access the collected data. End-users can log in to the system using their identity, and the level of access granted may vary depending on their role. For example, some end-users may have access to a limited subset of data, while others may be able to view and modify all data.

4.2. Categories of blockchain-based edge deployment

Blockchain deployment types for IoT systems can be classified into various categories depending on different perspectives. From the viewpoint of blockchain-based IoT systems, Wang et al. (2019) mentions two main architectures: IoT-involved blockchain and blockchain-as-a-service for IoT. In the former, IoT devices play a crucial role in the blockchain, while in the latter architecture, IoT devices do not participate in the blockchain organization. Another architecture consideration for a blockchain-based IoT system is presented in Dai et al. (2019), which proposes a blockchain-based IoT architecture with five layers: data, network, consensus, incentive, and services. Cloud servers or edge servers deploy full nodes, while the IoT layer performs light node tasks such as validation. Furthermore, both Reyna et al. (2018) and Saxena et al. (2021) mention the usage of blockchain in IoT with three types of architecture: IoT-IoT, IoT-blockchain, and hybrid approaches. These approaches involve end-to-end blockchains for blockchain management, storage levels for analytics and data storage, gateway levels for routing and local data gathering, site levels for user data generation, and device levels for device data generation.

The integration of blockchain and edge computing systems, as discussed in Yang et al. (2019), involves a hierarchy of systems with a general architecture for their cooperation. This architecture comprises two main components: (1) a private blockchain among edge nodes and end-users and (2) a public blockchain for a P2P network of servers. In the case of using a private blockchain within a hierarchy of edge nodes and end-users (1), there are two sub-categories based on the blockchain's maintenance. The first concept involves managing blocks formed and maintained only by edge servers. In contrast, the second concept involves end devices and edge servers participating in blockchain contribution by separating different tasks as light and main nodes. The second way of cooperation (2) involves using a public blockchain via a distributed blockchain cloud to maintain low-cost, security, and access to computing infrastructure from the perspective of P2P edge servers.

Our work expands upon prior research on blockchain-based edge architecture, such as Yang et al. (2019), by introducing a novel categorization of blockchain deployment types that consists of four types shown in Fig. 4. These types are discussed in detail as follows:

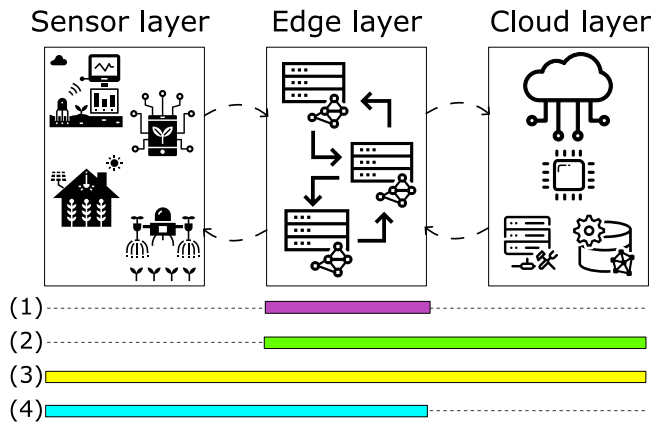

Fig. 4. A viewpoint of sensor–edge–cloud computing deployment: (1) full coupling of blockchain and edge layer, (2) coupling of blockchain and edge–cloud layer, (3) coupling of blockchain and sensor–edge–cloud layer, (4) coupling of blockchain on sensor–edge layer.

4.2.1. Full coupling of blockchain and edge layer

The complete deployment of blockchain at the edge layer involves implementing a specific blockchain protocol among edge servers. This approach enables blockchain to handle communication and data exchanges within the edge nodes, with edge servers acting as identical participants responsible for maintaining the blockchain protocol's functions. As a result, edge servers form a P2P network in a fully decentralized environment. Numerous studies (Nguyen et al., 2022, 2019; Gai et al., 2019; Lang et al., 2022; Xu et al., 2021a; Liu et al., 2021; Lin et al., 2021; Yang et al., 2021) have explored the deployment of blockchain technology in the edge layer as a platform for connecting and exchanging data among nodes.

Although the full coupling of blockchain and the edge layer offers openness in the system and the ability to attract a large-scale contribution, it requires substantial resources such as computation, communication, and storage for edge servers to manage the system. However, this approach is suitable for different types of blockchains. It allows edge servers to provide services based on specific applications requested by clients while maintaining connectivity among them using blockchain technology.

4.2.2. Coupling of blockchain and edge–cloud layer

Another interesting consideration for using blockchain at the edge is to combine it with cloud support from various usages (Nguyen et al., 2021b; Lu et al., 2022; Lee et al., 2020; Li et al., 2023; Bai et al., 2022; Zhang et al., 2021; Xu et al., 2022; Wang et al., 2021; Islam et al., 2021; Hu et al., 2021; Awad Abdellatif et al., 2021). This architecture aims to distribute the workload between the cloud and edge layers, resulting in improved performance due to reduced communication and storage. For example, in some studies (Lu et al., 2022), the cloud is responsible for maintaining backup storage for the system, while the edge servers manage blockchain responsibilities for secure connectivity among various devices (Nguyen et al., 2021b). In other cases, the cloud is used for robust computation, such as deep learning, while the edge servers maintain the blockchain as the system's database. Besides, Xu et al. (2022) describes using a key generation center as the cloud for blockchain updates, while edge servers manage the blockchain. Although certain studies design the deployment of blockchain at the cloud layer and then utilize edge servers for managing end-device connections, these approaches are out of scope for our consideration.

4.2.3. Coupling of blockchain and sensor–edge–cloud layer

Although sensors have limited resources, several studies (Li et al., 2021; Fan et al., 2021) have explored the use of blockchain in this layer.

However, these deployments require assistance from both cloud and edge layers. Current architecture designs propose a group of disjointed blockchains, where a set of connected sensor devices maintains each blockchain. This architecture is intrinsic to the coupling of blockchain and cloud–edge layers, where a main blockchain manages a set of sub-blockchains, connecting disjointed end-device blockchains to form a giant ecosystem. The two-layer blockchain system provides flexibility for customization in various use cases, such as permissioned or permissionless blockchain.

4.2.4. Coupling of blockchain on sensor–edge layer

In addition to the coupling of blockchain with the sensor–edge–cloud layer, some studies have also proposed the deployment of blockchain on the edge and sensor layers, as mentioned in Gumaei et al. (2021). However, the details of this approach are pretty ambiguous. The main objective of this deployment is to use at least two blockchains for the sensor and edge layers, similar to the coupling of blockchain with the sensor–edge–cloud layer, but without the use of the cloud layer. The goal is to increase the level of decentralization in the system.

4.3. Blockchain-enabled services in edge computing

A set of services based on blockchain technology can evolve traditional systems by providing a decentralized and trustless environment, especially traceability, data identity, device availability, and collaborative operations. Blockchain-based services can ensure data immutability, transparency, and security while minimizing the need for intermediaries. By leveraging blockchain's capabilities, these services can offer a transparent and tamper-proof system.

4.3.1. Data identity management or authentication

Although several studies mention a diverse range of services, including authentication, access control management, and identity management, we cluster these concepts into a single term known as identity management (Tobin and Reed, 2016; Dunphy and Petitcolas, 2018). This term encompasses the management of system participant identities, including edge servers and other entities, to guarantee security and prevent the entry of counterfeit entities. The success of identity management relies on a secure mechanism for providing and verifying identities for new members, along with the storage and management of these identities. The implementation of identity management enables other capabilities, such as authentication, authorization, and roles related to different duties in complex systems.

4.3.2. Device availability

Regarding the availability aspect, decentralization offers benefits of systems' fault tolerance. In a decentralized environment where identical edge servers are deployed, the availability of the system with a blockchain-based edge is ensured (Boudguiga et al., 2017). Even if there is a failure in the system or network, it does not affect the operation of the system, although it may impact performance.

4.3.3. Collaborative operation

One of the most appealing aspects of blockchain-based edge services is their ability to enable collaborative operations (Nguyen et al., 2019), particularly in the context of offloading (Feng et al., 2020). Offloading computing relies on adequate storage and computation capabilities, and resource management is often associated with offloading due to the similarity between resource orchestration and offloading. Offloading emphasizes the ability of network participants to assist in resolving requests, especially when a participant is unable to handle them. Accomplishing successful offloading requires synchronization of storage and computation among system participants for collaborative operation.

4.3.4. Traceability system

Blockchain's immutability feature allows for the implementation of traceability operations in systems (Tian, 2016), as it maintains a growing timeline of data without the possibility of late modifications. This turns the system into a trustable timeline machine, capable of providing audit services for tracing back history. As a result, the network participants store and capture the history of operations, enabling tracing and auditing. This feature enhances the system's transparency and trustworthiness, which are crucial for various applications, such as supply chain management and voting systems.

5. Security requirements of time-critical blockchain-based edge IoT applications

Various works have presented different security requirements for blockchain-based edge IoT applications from different perspectives. Authors in Wang et al. (2019) claim that privacy, identity and device management, and access control are critical security concerns for blockchain-based IoT applications. Similarly, authors in Xu et al. (2021b) discuss the security of blockchain-based IoT systems through the sensor, network, and application layers, and identify functional security features provided by the blockchain, such as privacy protection, access control, identity authentication, data assurance, anti-DDoS attack, and IoT network self-regulation. Lone and Naaz (2021) analyze several security-based applications for IoT, including authentication, authorization, access control, integrity preservation (data provenance, data integrity, and device integrity), secure data management, identity and key management, and non-repudiation. These studies emphasize the importance of integrating blockchain technology in IoT systems to address security challenges and provide secure and reliable IoT solutions.

Regarding security in edge computing systems, Yang et al. (2019) outlines various security challenges such as attacks in message transmission, data integrity, data leakage, unauthorized access, storage data reliability, and security of tasks offloading. This leads to security needs, including authentication, adaptability, network security, data integrity, verifiable computation, and low latency. Similarly, the analysis of blockchain-based EoT systems by Gadekallu et al. (2022) highlights the importance of secure services, such as access authentication, data privacy, attack detection, and trust management. By addressing these security concerns, blockchain technology can assist in the development of IoT and edge computing systems while enhancing trustworthiness and security. While previous works have recognized and explained the advantages of blockchain in forming blockchain-based services and using it as the core of these systems, they still lack a detailed analysis of the specific security demands in IoT and edge systems.

In order to provide a high level of security, all parts of an advanced blockchain-based edge IoT system need to be secured. Data transmitted over networks, including wireless communication and internet networks, must be secured and protected. In addition, data should always be available for authorized persons via a secure channel when needed. Furthermore, the system needs to guarantee that data must be properly used with the consent of the persons who relate to the data. To achieve the target, a system must fulfill ten security requirements: confidentiality, integrity, authentication, authorization and access control, privacy, trust, transparency, availability, automaticity, and tolerance. Detailed information on these requirements is discussed as follows:

5.1. R1-confidentiality

Confidentiality is a vital characteristic of any system, especially when dealing with personal data such as health status. All parts and participants of the system need to keep the collected data secure and cannot disclose the data without the permission of authorized persons. Only authorized parties and persons can access the collected data. In some exceptional cases shown as follows, data can be disclosed without breaching duties of confidentiality (General Medical Council, 2017):

- Data can be disclosed when the law requires, including the case when the courts allow disclosure of the data
- Data can be disclosed with the consent of the persons/ victims/ patients
- The process sets aside the common law duty of confidentiality
- Data can be exceptionally disclosed in some cases related to the public interest. However, the disclosure process needs to follow some particular requirements

To ensure a high level of confidentiality, IoT systems should apply the following strategies: data encryption, secure communication, secure storage, secure access control, device authentication and authorization, secure key management, regular updates and patch management, network segmentation, data anonymization, user education, monitoring, and intrusion detection. It is necessary to keep the IoT systems continuously monitored and updated.

5.2. R2-integrity

Integrity can be described as the overall completeness, accuracy, and consistency of data over its entire lifecycle. Data integrity can include many components, such as accuracy, security, and quality. When data has integrity, its stages, such as ready-to-use data, data in the transmit stage, data in the use stage, or data at the resting stage, cannot be edited by unauthorized parties. The benefits of data integrity are described as follows:

- Data is accurate and kept securely during its lifecycle
- Sensitive data is protected from being inappropriately stored
- The high speed and confidence level of data-driven decision-making are maintained
- Expensive audit trails to trace errors and recover data can be avoided or minimized
- High system performance can be maintained
- Data regulatory compliance can be properly guaranteed

To achieve a high level of data integrity, a system is recommended to carry out the following tasks: duplicated records/data elimination, improving data quality, focusing on data entry training to avoid human error causing data breaches and loss, updating regularly, and validating data and its source.

5.3. R3-authentication

Authentication is the process of recognizing and identifying a user's identity. In order to access data in an IoT system, an end-user needs to provide their credential (e.g., via a mobile app and a web browser) to the system. Each IoT system has its authentication type shown as follows:

- Single-factor authentication: this authentication method often uses the knowledge-based approach in which an IoT system relies on knowledge that an end-user knows or memorizes, such as PIN, password, or pattern, to verify the user's credentials. To achieve some security levels, strong passwords such as lengthy passwords with numbers, upper case, lower case, and special characters are required.
- Multi-factor authentication: this method represents two-factor, three-factor, and several-factor authentication. Two-factor authentication consists of two steps, including a knowledge-based authentication step mentioned above and a second verification step, while three-factor authentication has an extra verification step.

The IoT system should select appropriate authentication methods tailored to its architecture, user convenience, and specific system requirements. Some widely used authentication methods are shown as follows:

- Knowledge/Information-based method: in this method, the system can send a one-time PIN code or bar code via an email, a mobile phone, or a mobile app. An end-user will submit the received code to the system within a short time, such as 60 s for verification
- Token-based approach: the approach uses encrypted security tokens for verification of the user identity. In this approach, each request to a server includes a form of tokens that are verified by the server. Authentication tokens offer many advantages, such as (i) tokens are stateless and support scalability because it is not required to store session state in servers. The tokens consist of information that enables users to verify their identity without providing other information. (ii) Tokens have an expiration time. When the browsing session is finished and the service is logged out, the granted token is wiped out. (iii) Tokens are encrypted and unique to a user session. (iv) Tokens enable time-saving. A verified user does not need to provide their login credential again when the user re-visits a website.
- Device-based approach: this approach, which is one type of token-based approach, relies on physical devices containing tokens. An end-user must insert or place a physical device (e.g., a USB dongle or a smart card) into a USB port or a near-field communication reader. The system keeps track of the physical device to ensure that an authenticated user can access the system. When the session ends, the user must withdraw the device from the system. This method is more expensive but this achieves high levels of security
- Biometric-based approach: this method relies on a user's physical characteristics such as retinal, fingerprints, voice recognition, and face detection. Biometric verification methods are secure and convenient for users as it is unnecessary to carry physical devices. Nonetheless, biometric verification still has some drawbacks because fingerprint or voice needs to be shared with the system
- Certificate-based approach: this approach relies on a digital certificate acquired via cryptography for identifying a user. The certificate can be stored locally on the end user's computer. Therefore, it is not required to have a backup plan for lost tokens. Certificate-based approaches have several advantages, such as ease of deployment and management.

To ensure a high level of authentication, multi-factor authentication is often applied in many industrial organizations. Particularly, the first factor is often password-based authentication, and the second factor is knowledge-based authentication sent via a phone message or application. Some widely used authentication mobile applications are Microsoft Authenticator, Twilio Authy, and Symantec Vip Access. These applications often generate a one-time pincode which is valid only for 30 s. After the 30-second time expires, these applications generate a new PIN code. This mechanism improves the security level for authentication.

5.4. R4-authorization or access control

An authorization or access control is a process of providing user permission to access resources such as data, and virtual and actual devices. In many IoT systems, role-based access control, which defines different user roles such as administrators, internal users, external users, or guests, is applied. Each user can be assigned to a or several roles which allow the user access to corresponding and authorized resources. Attribute-based access control, which defines access policies based on attributes, such as user attributes, device properties, and time of day, is also applied.

In compliance with access control, data such as files can be classified into different categories. For example in governmental organizations, five levels including top secret, secret, confidential, sensitive, and

unclassified levels are used whilst in other organizations (e.g., private or public companies), four levels consisting of restricted, confidential, internal and public are often applied. Depending on the user role, a particular level can be accessed.

In addition to role-based and attribute-based access control, to ensure secure authorization and access control, it is recommended to apply some of the following strategies, such as least privilege principle, strong identity management, audit trails and logging, dynamic access control, periodic review and update access permissions, secure communication channels, user training, risk management, and emergency access procedures.

5.5. R5-privacy

Data privacy refers to the practices and guidelines aimed at ensuring that data is properly collected, handled, shared, and used while complying with applicable laws and regulations. Depending on the application, country, and context, different laws and rules may apply. For instance, the United States Health Insurance Portability and Accountability Act is a federal law that protects sensitive patient health information from being disclosed without the patient's consent or knowledge, while the Children's Online Privacy Protection Act focuses on the rights of parents to control data that websites can acquire from their children. In Europe, the General Data Protection Regulation (GDPR) provides citizens with the right to control their data. When a system needs to use information related to users, it is required to inform the user, for example, by popping up a form with the necessary information where the user can confirm the website's permission to work with the data, such as data manipulation, storage, and processing. The GDPR follows seven principles, which are as follows:[3]

- Lawfulness, fairness, and transparency: data is processed lawfully, fairly, and in a transparent manner
- Purpose limitation: data is collected for a specified and legitimate purpose. Data cannot be further processed for other purposes such as scientific or historical research
- Data minimization: an amount of collected data is adequate, relevant, and limited to the initial and specified purpose
- Accuracy: the collected data must be kept accurate and up-to-date
- Storage limitation: personal identifying data is stored as long as it is necessary for the specified purpose
- Integrity and confidentiality: appropriate security, integrity, and confidentiality must always be considered when data is processed. Cryptography algorithms for data encryption can be used to satisfy the consideration
- Accountability: GDPR compliance with these principles is demonstrated by responsible data controllers

With these acts and data protection regulations, privacy is highly ensured. Nowadays, this is almost a must to apply these regulations in IoT systems that involve human users.

5.6. R6-trust or confidence

Trust/confidence is a prerequisite in IoT blockchain systems. Confidence often relates to statistical evidence of how a system behaves, whilst trust is connected with the trustee's ability. Particularly, a trustee can be an end user/buyer who uses the services/products of a company and trusts the information the company publishes or guarantees. For example, a buyer trusts that a mobile phone produced by a well-known company has good quality and can be used reliably for a long period. Trust in IoT blockchain systems can be considered as the relationship between participated parties (e.g., end-users and service providers) in which one party voluntarily decides to rely on other parties and expects that all the jobs can be successfully done without any harm to the participated parties. With trust, tasks can be delegated to another third party, which helps achieve highly successful task completion (De Filippi et al., 2020). In contrast, confidence can be considered as an attitude of assurance in which one party or system ensures some success degrees to other parties for specific services in a particular context (Aldowah et al., 2021; Ion et al., 2008). Both trust and confidence can have different levels, such as low, medium, and high.

To ensure a high level of confidence and improve trust, it is recommended to apply the following strategies such as transparency and openness, third-party risk management, third-party validation and certification, regular updates and patch management, privacy protection, user education and training, regular security audits and testing, secure communication channels and regular communication with customers for the update notification, long-term support and customer feedback, and emergency response plan.

5.7. R7-transparency

Data transparency can be interpreted as the utilization of data must be carried out with integrity in which participants know which data is acquired, how data is processed, who has access to the data, and how the data can be interacted with. A decentralized network allows for distributed storing of data. Correspondingly, a single party cannot influence the stored data. According to Bertino et al. (2019), data transparency has many dimensions shown as follows:

- Utilization transparency points to the data usage, including data users, purposes of utilization, and processes
- Record transparency includes information such as time and location of data acquisition, sensor, and data storage
- Disclosure and data provision transparency relates to the data transmission between different organizations. This includes different aspects such as technical aspects, financial aspects, and legal aspects
- Algorithm transparency includes mechanisms, techniques, and algorithms for processing data
- Laws and policies transparency relates to regulations, policies, and laws associated with data
- Breach transparency consists of information related to a breach of data such as when the data is breached, which information is breached, where the breached data is stored, or which stage (e.g., draw data or encrypted data) the data belongs to
- AI ethics transparency relates to information extracted from the collected data or results from trained models using data

Blockchain technology can play a key role in transparency by requiring participants to exchange information to achieve a majority agreement on what is considered valid. Also, the confirmed information in blockchain requires tampers resistance, leading to greater transparency and traceability. To ensure a high level of transparency, in addition to using blockchain, it is recommended to apply the following strategies such as clear privacy and data sharing policies, data collection and security measures disclosure, granular user consent, data access logs, user feedback, and regular communication with users, third-party and open source software integration, regular privacy audits, and opt-in mechanisms ensuring that users actively agree to share their data.

5.8. R8-availability

Data must always be available and ready. When an end user needs to access the data from a system, the data must be available regardless of access time and location. However, it is challenging to maintain a high level of data available because of the following reasons:

[3] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

- Storage failure: it is possible that storage servers get scratched, and data cannot be accessed. This issue can be handled as the cloud service providers often offer solutions such as storing data in different racks and geographical places. When a rack gets scratched, the data is still available. However, it is not recommended to use centralized data storage as it still has many limitations, such as the risk of data loss, low-security level, and prone to data breaches
- Network failure or unstable network: when the network connection is not stable or interrupted, data cannot be properly accessed. The strong use of networks with redundancy options deals with network issues and ensures data availability. For instance, edge and fog computing help deal with these issues. Instead of getting data from cloud servers over the internet, data can be directly retrieved from distributed edge storage close to the end users
- Poor quality of data: when data is not completed, inconsistent, and redundant, poor quality of data occurs
- Data compatibility: data in one format in one specific environment may not be compatible with another; therefore, the use of a standard format for data is needed. For example, health data should be applied with the Health Level Seven standard, which is a set of international standards giving guidance with transferring and sharing data between different healthcare providers
- Security and data breach: access data can be blocked by malicious parties

In order to ensure a high level of data availability, it is recommended to apply the following strategies such as redundant data storage (e.g., in different distributed edge or fog devices), load balancing, the fail-over mechanism for automatically switching to backup systems, regular backups, continuous monitoring and alerting to notify of any anomalies, network redundancy, disaster recovery plan, user training and education, service level agreements, and proper documentations.

5.9. R9-secure automaticity

Automatic can be expressed as a process where actions can be made after some requirements are fulfilled. For example, an automated IoT system remotely collects data (e.g., humidity and temperature) from various sensors. When the soil is too grained, and its water level is lesser than some predefined thresholds, the system will automatically trigger a water pump for watering the soil with some predefined water levels. In blockchain systems, the smart contract is used to provide automaticity; particularly, when the requirements in a smart contract are fulfilled, actions (e.g., transmitting some tokens or executing a task) will be automatically carried out. However, these automated systems with smart contracts still have some security issues, such as reentrancy attacks, frontrunning, oracle manipulation, timestamp dependence, insecure arithmetic (e.g., integer overflow and underflow), denial of service, griefing and force-feeding.[4] These are discussed as follows:

- Reentrancy attacks: this kind of attack is a destructive attack in the Solidity smart contract. This attack occurs when a function in a smart contract calls to another untrusted contract that then calls back to the original contract. This mechanism can cause a security leak. For example, the Decentralized Autonomous Organization attack is a well-known reentrancy attack that caused a loss of many million US dollars recently. Reentrancy can consist of reentrancy on a single function and cross-function reentrancy. In order to protect smart contracts against reentrancy attacks, it is recommended to utilize function modifiers that not only prevent reentrancy but also ensure all state changes are completed before external contracts are called
- Frontrunning: when a transaction is submitted to the blockchain, the transaction is brought to the memory pool and waits for inclusion into the next block. At this phase, the transaction is visible to observers of the network. Once the untrusted actor finds a transaction in the pool that the actor can exploit to get profits, the actor can copy and manipulate the transaction, and then submit it with a higher gas fee. Correspondingly, the manipulated transaction will be included in the next block. Frontrunning is an issue on public blockchains like Ethereum. One of the best approaches to deal with front running is polishing the importance of transaction ordering or time
- Oracle manipulation: some smart contracts may require data from external sources outside the blockchain network. In this case, oracles are responsible for feeding external data outside of the blockchain network to smart contracts in a secure way. It is possible that Oracle is manipulated by an untrusted party, which causes some vulnerabilities such as some actions are still automatically carried out even though incorrect data is provided. The easiest way to deal with oracle manipulation is to use decentralized oracles like Chainlink (2023), Tellor (2023), or Witnet (2023). Using a combination of multiple oracles increases security since it is harder to attack all these oracles. Another solution to overcome oracle manipulation is to use a time-weighted average price feed that is the average of periods and all oracles
- Griefing: a gas griefing attack occurs when the amount of the required gas is sent to execute the smart contract but cannot satisfy the smart contract's sub-calls to other smart contracts. In this case, two options including reverting the whole transaction and continuing execution can occur, which attackers can exploit to censor transactions. One way to deal with griefing is to carefully implement logic that requires forwarders to provide sufficient gas to complete the sub-calls. Another way is to allow only trusted parties who relay a transaction
- Timestamp dependence: Miners can manipulate the timestamp of the block to attack the smart contract. Therefore, it is recommended to consider direct and indirect usage of timestamps. To prevent this attack type, it is suggested to avoid using block.timestamp. In case block.timestamp is used, the 15-second rule must be followed. Particularly, the 15-second rule mentions "if the scale of your time-dependent event can vary by 15 s and maintain integrity, it is safe to use a block.timestamp"
- Insecure arithmetic: it is necessary to consider the data types used in smart contracts. For example, small data types such as int8, uint8, int16, and uint16 can easily reach their minimum and maximum values. As a result, arithmetic underflow and overflow can occur. In order to prevent arithmetic underflow and overflow, it is recommended to use the functions in the SafeMath library offered by Openzeppelin (2023), which is a well-known company in the blockchain industry dealing with smart contracts. The library will take care of underflow and overflow in subtraction, division, addition, and multiplication
- Denial of service (DoS): DoS restricts authorized users from using the smart contract for a period or even permanently. There are three well-known types such as unexpected revert, block gas limit, and block stuffing. One of the solutions dealing with DoS is to use a pull model instead of a push model

In addition to the smart contract, to ensure secure automaticity, it is recommended to apply the following strategies such as intrusion detection and prevention to automatically monitor network traffic and identify suspicious activities, regular security audits for identifying weaknesses in the automated processes, automated patch management for updating with the latest security patches, containerization and virtualization for automatically restarting and maintaining services.

[4] https://consensys.github.io/smart-contract-best-practices/attacks/

5.10. R10-tolerance

Fault tolerance is one of the most crucial features of smart systems such as smart health, SaR, and vehicles that deal with human health and life. Particularly, smart systems are able to carry out their tasks properly even though there are some errors or unexpected abnormalities. For example, when cloud servers do not properly respond, the system should be able to carry out tasks locally at the edge and provide real-time analytic results. In some cases, when sensor devices malfunction, the system should be able to detect the improper sensor devices and inform the system administrator about the situation. This can be carried out via the malfunctioned sensor device detection and push notification service supported by edge or fog computing. In summary, to ensure a high level of tolerance, it is recommended to apply the following strategies such as redundancy in all levels including hardware, software, and network, fail-over mechanisms for switching to backup systems and automated recovery, distributed storage, load balancing, continuous monitoring and alerting, resilience testing, emergency power, and environmental controls, caching and data replication and synchronization, containerization, and virtualization.

In order to satisfy the above ten requirements, it is suggested to consider all aforementioned strategies. Fortunately, many of the mentioned strategies do not have conflict, which leads the implementation to become less challenging. In case there are conflicts, it is recommended to apply other strategies which provide the same effectiveness.

6. Blockchain-based edge IoT potential usages

Regarding the application perspective, the usage of blockchain enables manageable and collaborative services to traditional systems, including integrity management, availability, collaborative operation, and traceability. The section details potential and state-of-the-art application domains pondered with a blockchain-based edge by communities.

6.1. Smart healthcare

Smart healthcare, including remote health monitoring, is widely used in many places and normally refers to the use of technology and data analytics to improve the quality, efficiency, and accessibility of healthcare services. It includes a range of innovative technologies such as telemedicine, wearable devices, mobile health apps, and AI that can help monitor, diagnose, and treat patients remotely and more effectively. However, the existing smart health monitoring systems often have some challenges, such as issues related to security, reliability, real-time requirements, and fault tolerance. The proposed system architecture, as depicted in Fig. 5, helps overcome the limitations of the traditional healthcare system and improve the delivery of healthcare services. The illustrated architecture is composed of five primary layers, including the data generator layer or sensor layer, edge layer, blockchain layer, cloud layer, and application layer.

The first layer is the data generator layer, or sensor layer, which is responsible for acquiring data from various sources (e.g., from a human body or from surrounding environments). Particularly, wearable or implantable devices can collect different types of e-health data including low and high data rates such as ECG, EMG, EEG, EOG, Oxygen saturation, glucose levels, and body temperatures. These devices require specific configurations, including varying channel numbers, the number of samples per second per channel, and data resolution, depending on each e-health application. For example, an ECG monitoring app would necessitate 1, 3, 6, or 12 channels with a data rate of 250 samples per second per channel to achieve high-quality data. Wearable sensors are often equipped with a Lithium battery which is often less than 1000mAh to ensure small sizes and low weight. On the other hand, fixed sensor devices can be responsible for acquiring contextual data, such as room temperature, humidity, and air quality. The fixed devices are often supplied by a wall-socket power supply. The combination of e-health data and contextual data helps improve the accuracy of disease diagnosis. The captured data can be either preprocessed or kept intact before being transmitted wirelessly via an edge gateway to edge servers for further processing and analysis. In many health monitoring applications, data can be merely processed on wearable devices with simple algorithms, such as moving average filters or low-pass filters. This helps improve the energy efficiency of wearable devices in many cases because transmitting large data consumes large energy. As mentioned, AES-256, which operates on fixed-size blocks of data (e.g., 128-bit length), can be applied to wearable devices to protect the data transmitted over the network. The increased latency caused by applying AES-256 on an 8-bit 16MHz AVR micro-controller is small around 170mus and 150mus for encryption and decryption, respectively (Nguyen Gia et al., 2017). In addition, the average power only increases by 2 mW. These small increased power consumption and latency do not cause dramatically negative impacts on the sensor devices and the system latency. Therefore, AES-256 can be applied for time-critical healthcare applications such as ECG, EMG, and EEG monitoring which allows a maximum latency of a few hundred milliseconds (e.g., 500–700 ms).

Wearable devices often use low-power wireless communication protocols such as nRF24, 6LoWPAN, and BLE5 to achieve energy efficiency. Particularly, these protocols can be used for fall detection, heart rate monitoring, body temperature, and glucose monitoring applications that do not require high data rates. BLE5 can be also used for ECG and EMG monitoring applications using several data acquisition channels in which each channel can collect 150 16-bit samples/s. This data rate is often applied for ECG monitoring in ambulances. For specific scenarios, when higher data rates (e.g., 250 samples/s per channel) and multiple channels such as 15 channels are needed, BLE5 can be customized to support the data rate of 2Mbps. In such cases, the increased current consumption can be around 3–6 mA when switching from 1Mbps to 2Mbps. In practice, instead of operating with 2Mbps, the maximum data rate is around 1.3–1.4Mbps. When much higher data rates such as thousands of samples per second for multiple channels, Wi-Fi can be selected. However, applying Wi-Fi can increase the average power consumption to around 50 mA or even more when compared with BLE5. Therefore, to achieve a high level of energy efficiency, it is recommended to select suitable wireless communication protocols with proper configurations for sensor devices.

The second layer is the edge layer which includes edge devices (e.g., gateways, routers, and servers) deployed at the edge of the network. To be specific, the edge gateway is responsible for receiving data from sensor devices and transmitting the data to edge servers. The gateway can also support computations, such as data filtering and processing. Typically, a gateway is placed at a room corner or corridor and uses power from wall sockets. From that, in large monitored areas like homes or hospitals, multiple gateways can be deployed. To provide high-quality edge services that meet stringent real-time requirements, it is important to consider the location where computations should be carried out (e.g., edge, cloud, or hybrid of edge and cloud). In this regard, both computation and transmission latency should be taken into account, as expressed by the following formula (Eq. (1)). The data will be operated at the gateway if the total latency of processing raw data at the edge gateway and transmitting the processed data is less than the total latency of the same process at the edge server and vice versa. In some cases, when an algorithm or a service involves different computations, it is recommended to divide the algorithm into smaller tasks, where each task applies the discussed formula to decide the processing location.

$$R = L_{p_r d_g} + L_{t_p d} - (L_{t_r d} + L_{p_r d_s}) \tag{1}$$

$$\text{Location} = \begin{cases} \text{Edge gateway}, & \text{if } R \geq 0 \\ \text{Edge server}, & \text{otherwise} \end{cases}$$

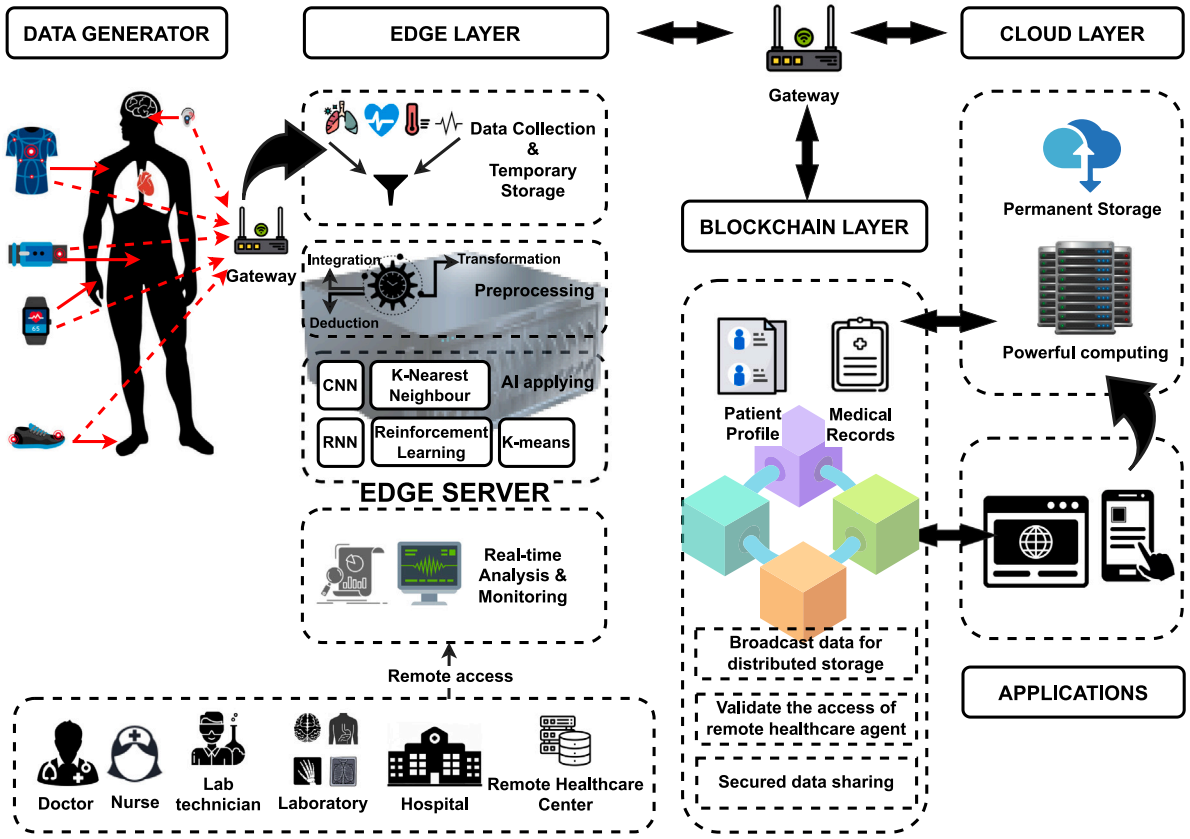

Fig. 5. Blockchain-based Edge-IoT system in smart healthcare application.

where $L_{p_r d_g}$: processing raw data at the gateway, $L_{t_p d}$: transmission of processed data, $L_{t_r d}$: transmission of raw data, $L_{p_r d_s}$: processing raw data at edge server, R : comparison latency result.

In the context of smart homes and clinics, the number of applied edge servers is dependent on the application requirements. These servers offer a multitude of benefits such as running complex algorithms, enabling distributed data storage and processing, and facilitating machine learning and deep learning models, e.g. Convolutional Neural Network (CNN), K-nearest neighbor, K-means, and LSTM for disease detection and classification. Edge servers can also be connected to monitors which doctors, nurses, or caregivers can use for real-time monitoring. Notably, each edge server here can act as a blockchain node that can add blocks having smart contracts into the blockchain network. Smart contracts can be employed to buy specific medical resources when they are not available in the facility. For instance, when a particular blood type is urgently required for an operation, but the clinic does not have enough units of the blood type, a smart contract can be utilized to request the required blood type from suppliers or nearby hospitals. Any participating supplier that satisfies the requirements of the smart contract can automatically provide the blood to the clinic. All different parties, such as hospitals, public sectors, and public authorities can join the blockchain network.

The cloud layer consists of servers offering advanced cloud services, such as big data analytics. Cloud servers are also used to train deep learning models, such as cardiovascular disease detection and prediction models based on CNN. Once the models are trained, they are transmitted to edge servers for real-time classification. In the proposed system architecture, cloud servers can receive data directly from the edge layer without going through the blockchain network. In this case, cloud servers store streaming and pre-processed data transmitted from the edge servers to enable real-time monitoring, with a strict time requirement measured in milliseconds. To maintain some levels of security, data in cloud servers can be purged after a few minutes. Meanwhile, edge servers also add data to blocks of the blockchain network. From that, when remote users, such as caregivers and medical doctors, want to access real-time e-health, they can use a mobile app or a browser belonging to the applications layer to connect to cloud servers. In this case, blockchain can be used with a credential verification mechanism at cloud servers for access validation. Historical data can be retrieved from the blockchain network depending on the scenario. It is noted that the presented architecture shown in Fig. 5 can be customized and expanded. For example, an extra intermediate layer, such as fog, can be added between the edge and the blockchain layers to offer fog services that help achieve bandwidth conservation and improve response time.

6.2. Smart grid

The smart grid system represents an advanced infrastructure for power distribution that leverages modern communication and technology to enhance the efficiency, reliability, and sustainability of the traditional power distribution network. To be more specific, traditional power grids operate as a centralized control center with power flowing unilaterally from power plants to consumers, which results in several limitations. In practice, a typical grid system involves various entities in the generation and distribution of energy, such as power plants, renewable energy sources, e.g., thermal, solar, wind, hydrogen, distribution companies, and end-users or consumers. These entities generate, consume, and exchange energy in a complex way, making it difficult to track and manage energy transactions. The situation is further compounded when the distribution system operator needs to coordinate many consumers and producers in the network while accounting for the intermittency and uncertainty of various distributed energy resources (Khan and Masood, 2022). To address these limitations, nowadays, smart grids should be designed as a two-way system where the flow goes from customers back to the grid. This can bring

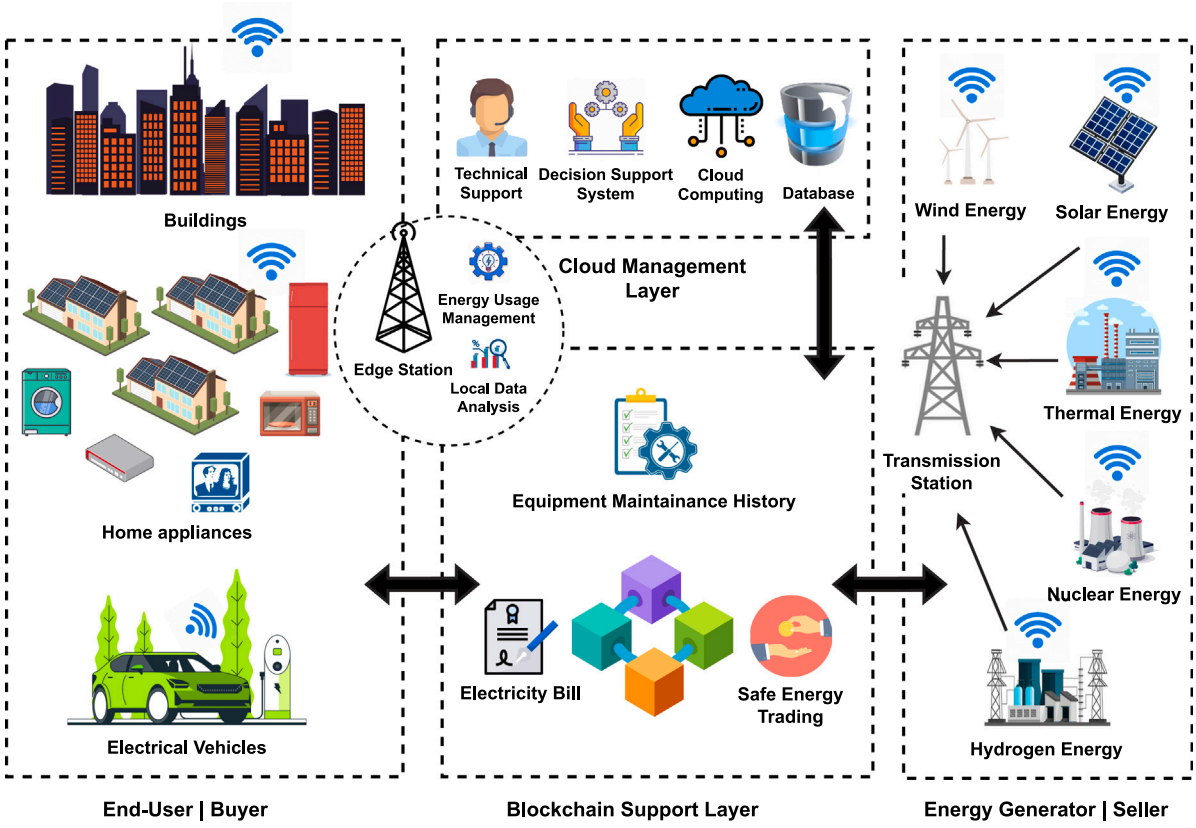

Fig. 6. Blockchain-based Edge-IoT system in smart grid application.

flexibility, resilience, and adaptability to changing energy needs and demands.

Over the years, the smart grid system has undergone significant evolution, and the emergence of blockchain technology has presented new opportunities for managing power grids. Fig. 6 illustrates the proposed system architecture, which is based on a two-way system design concept. Specifically, it encompasses a large-scale collaborative system comprising decentralized blockchain networks, edge computing, and AI to overcome the aforementioned limitations. In this architecture, end-users embody the consumer entity, which can be a smart home, a building, or an electric vehicle. These entities are equipped with internet connections to enable seamless communication with the nearest edge server, facilitating the purchase and consumption of energy from energy generators or control stations. Information related to energy consumption and harvesting can be updated in this way with a low frequency, such as one update per few minutes.

The edge servers, interconnected via the edge gateway, have been equipped with robust hardware to execute algorithms and provide edge services. In addition, these servers also serve as blockchain nodes that can add data to blocks with smart contracts.

The blockchain layer is a fundamental component consisting of blockchain networks, nodes, and blocks that execute smart contracts. These blocks play an essential role in energy trading, which reduces costs and saves energy when energy trading between entities can be done automatically. Besides, energy transactions can be recorded securely and transparently, creating a tamper-proof ledger that all participants in the system can access. The blockchain nodes also verify and validate each energy transaction, ensuring the accuracy and integrity of the information accessible to all participants in the system.

The cloud management layer consists of cloud servers for offering different cloud services, including AI-based solutions. It is noted that the cloud layer of the smart grid system is only connected to the blockchain network. This leverages the benefits of decentralized infrastructure. This makes the system architecture different from those used for time-critical healthcare applications.

Finally, a potential use case that aligns with our proposed two-way system design involves a solar power plant that generates electricity and sends it to the grid, which is subsequently transmitted to a distribution company for allocation to households and businesses. For each time the energy is transferred between entities, a smart contract is executed on the blockchain, recording the details of the transaction, including the amount of energy transferred, the time of the transaction, and the price paid. End-users can also use the system by generating their own energy through renewable sources, such as rooftop solar panels. The surplus energy produced can be sold back to the grid, with the blockchain recording the transaction details.

6.3. Smart maritime search and rescue

SaR is a critical coordinated effort to locate and aid individuals in danger or missing in different environments or locations, such as forests, mountain ranges, caves, or seas. This system often involves multiple organizations, such as emergency services, government agencies, and non-governmental organizations, and can involve a range of resources, including aircraft, healthcare, ground teams, specialized equipment, and trained specialists. Besides, different flying resources are used depending on the size of the search area, terrain, weather conditions, and resources available. However, drones (UAVs) have been increasingly used in this activity in recent years due to their numerous benefits. To be more specific, drones can provide more close-up imagery and detailed information, particularly in remote or inaccessible places such as mountain ranges or forests, where ground access is limited. They can cover an adequate search area and reach locations that other vehicles or humans cannot easily access in a short period (Qingqing et al., 2020). In cases where the number of victims is large and scattered across different areas, several drones

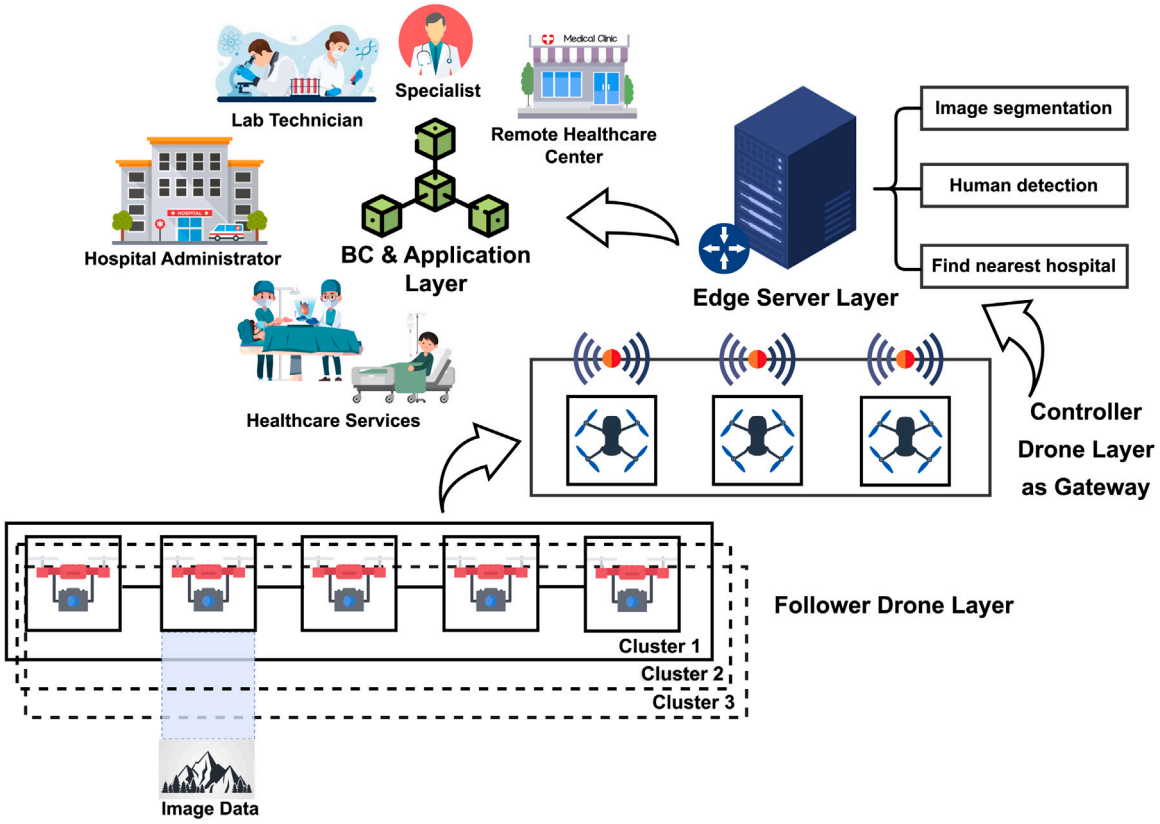

Fig. 7. Blockchain-based Edge-IoT system in Search and Rescue application.

or a swarm of drones can be used simultaneously. Nonetheless, along with these mentioned advantages, drone-based systems for SaR still have many drawbacks that must be addressed. For instance, as drones are commonly controlled by members of rescue teams, who manually monitor the streaming data from captured images and videos, using multiple drones requires additional team members to manage these devices. This could pose difficulty in some urgent cases. Furthermore, it can be a challenge to properly detect victims when relying solely on streaming video, particularly in adverse conditions such as low light and inclement weather. Thus, advanced drone-based systems for SaR are necessary, which can autonomously search large areas in minimal time and detect victims in harsh environments, e.g., nighttime or heavy rain weather. These systems must provide high-quality services and security while working with the rescue team to improve the chances of locating victims. It is important to note that SAR systems do not replace the role of the rescue team; rather, they offer support to increase the possibility of finding victims. The proposed system architecture, shown in Fig. 7, overcomes the existing challenges and fulfills requirements R1 through R10 while improving the quality of services. The system architecture comprises a follower drone layer, a controller drone layer, an edge server layer, and a blockchain and application layer.

The follower drone layer includes multiple small drones equipped with various types of cameras, including RGB and thermal cameras, that enable capturing videos at nighttime. These drones can also serve as wireless communication bridges, extending the communication range in certain scenarios. On the other hand, the controller drone layer consists of bigger drones that function as an edge gateway, providing support for multiple edge services and transmitting data between small drones and an edge server placed on a rescue vehicle, e.g., a boat or aeroplane. In addition, a big drone also acts as a swarm leader, sending commands to control its members, while small ones are members of the swarm.

The main differences between the small drones in the follower drone layer and the big drones in the controller drone layer are as follows: (i) a big drone is often more expensive and supports a higher load capacity, which allows the integration from different types of sensors such as Lidar, cameras, and a powerful edge computer; (ii) a big drone is physically bigger and can accommodate bigger battery packs than the small one. Small and big drones can be specifically customized depending on the application. Besides, rescue vehicles with powerful edge servers can provide advanced capabilities like distributed data storage and geographical location awareness. When the search areas are extremely large, and the number of victims is high, several rescue vehicles with edge servers can be used. The edge layer in Fig. 7 can contain multiple edge servers acting as blockchain nodes. The blockchain network can be private or public; however, a private one, such as Hyperledger Fabric, is preferred due to its permission features. Participants in these networks can range from public authorities and healthcare specialists to hospitals. The leverage of blockchain in this edge IoT system is mainly for enhancing the security and automaticity of the SaR services. In particular, this architecture provides tamper-proof and transparent records of all the collected data, access to authorized parties only, and resistance to any single point of failure. More importantly, it enables faster and better coordination with automatic triggers based on predefined rules using smart contracts. This could be simply as alerting the rescue teams when a missing person is detected in a particular location. Finally, a similar system architecture was recently proposed in Nguyen et al. (2023a), demonstrating the effectiveness of the proposed design in improving the quality of SaR and healthcare services.

7. Motivation and related work

This section presents a comprehensive overview of the latest cutting-edge survey on the integration of edge computing, edge AI, IoT, and blockchain technology.

7.1. Survey on systems using IoT and edge

This subsection provides an overview of surveys and reviews on the integration of edge computing into IoT systems. In Yu et al. (2017), the authors highlight the benefits of edge computing-based IoT architectures in overcoming the limitations of conventional IoT systems. However, the authors note that despite the potential advantages of edge computing, challenges such as standardization, resource management, and security and privacy still exist due to the diverse layers and attack objectives in IoT systems.

In Omoniwa et al. (2019), the authors present a comprehensive survey on the application of fog and edge computing for IoT, focusing on service, architecture, and security aspects. They compare edge-based IoT architecture with traditional cloud-based IoT architecture in terms of storage, network, computation, and service discovery. Although there is no clear distinction between edge and fog computing, the authors note that edge computing addresses resource contention in the things domain, while fog computing is more concerned with infrastructure. The authors analyze three abstract architecture types, *application-network-sensor*, *application-service-network-sensor*, and *business-application-service-network-sensor*, along with potential protocols and technologies. Additionally, they discuss different simulation tools and security issues associated with fog and edge computing in IoT systems.

In Laroui et al. (2021), a comparison and analysis of cloud and edge computing in IoT applications, such as smart cities, smart homes, smart grids, healthcare, and smart vehicles, is presented. The authors discuss various services, including task scheduling, software-defined networks, and security. They also summarize the contributions of current edge computing for IoT via QoS metrics and security concerns, as well as future directions and learned lessons.

In Kong et al. (2022), a survey of edge computing integrated into IoT is presented. The authors discuss the limitations of previous studies in system architecture, the benefits and potential challenges of edge computing in IoT systems, and present and analyze a taxonomy of edge computing in IoT. The taxonomy includes architecture, operating system, communication protocol, computing, security, and application. Finally, the authors discuss challenges and learned lessons, such as standardization, orchestration of resources, development tools, security, and privacy.

In Ray et al. (2019), the authors present a taxonomy of the edge-IoT ecosystem based on resource types, including computation platform, data management, and communications. The article also covers related software, analytics, and system-on-chip platforms. The authors propose a novel e-healthcare architecture as a case study for analyzing the architecture, capabilities, and future directions of the edge-IoT ecosystem.

In their survey, Fazeldehkordi and Grønli (2022) provide a comprehensive comparison of various computing paradigms, including cloud, mobile, fog, and edge computing. They also discuss security and privacy challenges associated with edge computing and present several solutions to address these concerns. Additionally, the authors review different architectures for edge computing-based IoT and highlight the key challenges that need to be addressed to facilitate the widespread adoption of this technology.

Sarker et al. (2019) present a survey that focuses on various edge-IoT applications, such as smart cities, industrial IoT, smart metering, and environment monitoring, and how they can be implemented using LoRa technology. The authors explain how LoRa can facilitate communication between edge and cloud computing environments, and how it can be leveraged to enhance the performance and efficiency of these systems.

The convergence of edge, fog, and cloud computing is discussed in the survey by Firouzi et al. (2022). The authors highlight the importance of resource management in this context and the potential of AI-enabled IoT to improve the performance of edge-fog-cloud systems. They also discuss the security and privacy challenges that need to be addressed to ensure the success of these technologies.

Discussing trust edge-based IoT architecture, Fotia et al. (2023) investigate trust decentralization from edge-based IoT architectures, especially the usage of blockchain. The survey emphasizes the key research questions, including architecture for edge-based IoT, the framework for trust with reputation technique, a blockchain solution for edge-based IoT architecture, and the performance for trust evaluation. The authors discuss the difficulties in comparison due to the various blockchain usages, but most cases are based on performance.

7.2. Survey on blockchain and IoT

Regarding some drawbacks of IoT, while it enabled conventional devices to become smart and autonomous, existing IoT systems are still limited in security, privacy, and reliability as they rely on centralized cloud servers. To address these issues and improve the quality of service, one solution is to incorporate blockchain technology, which offers distributed storage and non-tamperability.

The survey conducted by Huo et al. (2022), Wang et al. (2020) focuses on the challenges faced by IIoT systems and the potential benefits of integrating blockchain technology. The authors highlight the key features of blockchain, such as distributed storage, non-tamper proof, decentralized credit, and stability and efficiency of essential services, that make it a promising solution for addressing the challenges of IIoT. However, the analysis of system architecture and security is not thoroughly addressed in these surveys, despite the careful presentation of advantages associated with blockchain-based IIoT applications.

In Wang et al. (2019), the authors present a survey of blockchain-based IoT architectures that address the issues of malicious behavior in devices and incorrect sensor data. The survey also analyzes the challenges related to computation, communication, energy, storage, and mobility when integrating Blockchain into existing IoT systems. Furthermore, the authors demonstrate that integrating blockchain into IoT systems creates many opportunities, such as incentive strategies using tokens, smart contracts for autonomous execution, and secure services.

In Reyna et al. (2018), the authors present a survey highlighting the security challenges of IoT and propose the integration of blockchain into existing IoT systems to leverage decentralization, identity, autonomy, reliability, and security. Inspired by this work, Saxena et al. (2021) provide a survey that introduces blockchain-based systems with security interoperability, autonomous interaction, reliability, source code deployment, service market, and traceability. These systems address the challenges of IoT systems and enhance the quality of service. The survey also analyzes the integration trends of IoT with blockchain and represents relevant blockchain-based IoT applications and future research directions.

In Dai et al. (2019), the authors provide a comprehensive survey that focuses on the integration of IoT and blockchain. The survey first discusses the challenges of IoT, including privacy and security vulnerabilities, and the advantages of blockchain, such as decentralization and immutability. Then, the survey investigates the integration of blockchain and IoT that enables different merits, such as interoperability, traceability, reliability, and autonomic interaction. Furthermore, the authors present issues when using blockchain together with 5G and IoT. Finally, the survey discusses some future research directions to promote the development of blockchain-based IoT systems.

In Xu et al. (2021b), the survey focuses on the security risks of IoT and introduces the characteristics and classifications of blockchain-based IoT security. Furthermore, the survey discusses the challenges of blockchain-based IoT systems, attacks, and information-sharing security, as well as research trends, such as blockchain with 6G.

In Lone and Naaz (2021), the review analyzes existing works using blockchain and smart contracts to secure IoT systems. The review categorizes the works based on key findings, blockchain platforms used, application domains, and security services provided. The paper concludes by discussing the challenges and future research directions in this area.

7.3. Survey on blockchain and edge computing

The integration of blockchain technology into edge computing systems is motivated by the need for increased security, particularly the benefits of decentralization. Similar to IoT ecosystems, the heterogeneous connectivity among end devices is a critical concept; however, the lack of security and horizontal scalability can hinder the development of these systems. Therefore, recent works in edge computing are leveraging blockchain technology to provide solutions for these challenges.

In Yang et al. (2019), a survey focuses on the integration of blockchain and edge computing in the context of the IoT. The survey starts with the motivation and advantages of integrating blockchain and edge computing, such as security, reliability, and efficiency. The authors then present different blockchain-based edge computing architectures and discuss their benefits and challenges. In addition, the survey analyzes the potential applications of blockchain-based edge computing in various IoT domains, such as smart homes, smart cities, and healthcare. The authors also discuss the challenges and research opportunities in this field, such as resource management, scalability, interoperability, and standardization. Finally, the authors summarize the state-of-the-art research and provide insights into future research directions.

Starting from the limitation of Edge Intelligence (EI) via computation, storage, and model, Wang et al. (2022b) points to the need for solutions in management and security with blockchain technology in computation, data transmission, and model optimization. In detail, the issues in the computation of EI include the management of heterogeneous computing, the lack of power computation, and the need for hardware security. Regarding data transmission at the edge layer, edge servers play around the network edge, which leads to latency in communication among them and also security issues related to data administration; meanwhile, the model training at the edge layer enables vulnerabilities.

In their review article Gadekallu et al. (2022), the authors discuss the integration of blockchain and Edge-of-Things (EoT) in various industrial applications, including smart cities, smart grids, smart homes, smart transportation, and smart healthcare. The article highlights the potential benefits of this integration and analyzes the security challenges faced by blockchain and edge-based IoT systems, such as access authentication, data privacy, attack detection, and trust management. The authors also present research challenges and future directions to advance this field.

7.4. Motivation and contribution

Table 3 summarizes recent literature reviews and surveys based on five main features, including scope, primary contributions, security service, future direction, and major applications. Given that the system architectures and security-related concerns of blockchain-based edge IoT systems were not thoroughly examined in these discussed studies. In this paper, we offer a more in-depth study by providing a comprehensive system architecture that integrates all relevant technologies and concepts, including blockchain, edge computing, Edge-AI, and IoT. Furthermore, our article comprehensively discusses vital security requirements that impact the quality of service of blockchain-based edge IoT systems. These security requirements include confidentiality, integrity, authentication, authorization/ access control, privacy, trust/confidence, transparency, availability, secure automaticity, and tolerance. In addition, while other blockchain review articles did not analyze the blockchain deployment types with respect to the system architecture, this article not only presents four main blockchain deployment types but also discusses the advantages and disadvantages of each type. Lastly, this article presents opportunities and open directions for future development.

8. Discussion: Considered issues and future trend

In this section, we discuss two important topics that greatly impact the quality of service: the performance quality and reliability of a blockchain-based edge IoT system. These topics include the blockchain deployment types in a blockchain-based edge IoT system and the security levels of a blockchain-based edge IoT system. Then, this section discusses potential applications where a blockchain-based edge IoT system can be applied to enhance the quality of service.

In the blockchain deployment type, four types shown in Fig. 4 are compared and analyzed to determine advantages and disadvantages. This helps readers choose suitable deployment types for each specific application. In addition, ten important security requirements mentioned in Section 5 are used to investigate the reliability and security of a blockchain-based edge IoT system. With the system security level inferred from the number of security requirements that the system architecture can and cannot fulfill, we also suggested and discussed some useful techniques and approaches to improve security while not infringing on other application requirements.

In order to have a fair assessment, state-of-the-art works using edge computing and blockchain are compared with the developed blockchain-based edge IoT system, shown in Table 4. The comparison includes some specific points, such as blockchain type, the blockchain deployment, the number of fulfilled security requirements, and the applications.

8.1. Blockchain deployment types

As mentioned, blockchain deployment types are classified into four types. The pros and cons of each deployment type are discussed as follows:

8.1.1. Full coupling blockchain and edge layer

The proposed architecture offers multiple security benefits, particularly in terms of ensuring availability and single-point tolerance in the event of system crashes or the presence of Byzantine participants. An additional advantage is its open platform, which facilitates collaboration and trust-building among participants through unique data storage and management capabilities. However, implementing blockchain technology at the edge layer poses performance challenges, including low throughput and high storage capacity requirements due to the replication of data and communication among numerous blockchain participants.

8.1.2. Coupling blockchain and edge–cloud layer

By leveraging the vast resources of cloud computing, the performance of full coupling blockchain at the edge layer can be significantly improved. Cloud computing can serve as a trusted intermediary, managing administrative tasks like bootstrapping, identity verification, and certificate generation, leading to an overall better blockchain deployment performance. However, this approach introduces additional drawbacks of reducing the level of decentralization, leading to single-point failures caused by the cloud. To address this concern, it is essential to carefully decouple the responsibilities between the cloud and edge layers, mitigating the risk of single-point failures while maintaining optimal performance.

8.1.3. Coupling blockchain and sensor–edge–cloud layer

The deployment of blockchain technology at the edge and sensor device layers offers a better way for decentralization, eliminating the need for trust in a single component and reducing reliance on cloud computing. However, this viewpoint requires further examination in real-world usage cases due to several challenges and limitations that need to be considered. For example, managing the diversity of blockchains in a coupling blockchain and sensor–edge–cloud layer can pose

Table 3
A summary of similar works in blockchain-based edge IoT.

Work	Scope	Main contribution	Security service										Key future direction	Major applications
			R1	R2	R3	R4	R5	R6	R7	R8	R9	R10		
Yu et al. (2017)	How edge boosts IoT	Pros & cons in edge computing Security & performance in IoT Issues in edge IoT											System integration Resource management Security and privacy Advance communication	Smart grid Smart city Smart transport
Omoniwa et al. (2019)	Edge/fog-based IoT	Fog-edge IoT in architecture Various comparison in simulations Various usages & potential directions	✓	✓	✓	✓	✓	✓		✓			Interface & Coordination Simulation capability Mobility & scalability Virtualization in resources	Smart transport Smart grid Smart healthcare Smart city
Laroui et al. (2021)	Edge/fog-based IoT	Concepts in edge-fog-cloud Various usages with edge IoT Security & privacy in edge IoT		✓	✓								Scalability Availability & mobility Security and privacy Intelligence at edge	Smart city Smart transport Smart grid Smart healthcare
Kong et al. (2022)	Systematic edge-IoT	Integration of edge IoT Lesson learned with pros & cons Aspects of edge IoT			✓	✓	✓					✓	Security and privacy Heterogeneous platforms Task allocation Tools for edge-IoT	Smart city Smart healthcare Mobile VR and AR Industrial applications
Ray et al. (2019)	Industrial edge-IoT	Industrial standard in edge computing Components of edge IoT											Edge architecture Blockchain usage	Healthcare Industrial applications
Fazeldehkordi and Grønli (2022)	Edge paradigms	Security issues in edge computing Pros & cons in architecture	✓	✓		✓	✓	✓		✓		✓	Security threat Authentication Authorization	Public transport
Firouzi et al. (2022)	Edge-fog-cloud in IoT	SOTA edge-fog-cloud IoT architecture Offloading in edge-fog-cloud											Resource management Failure management Collaboration Performance	Smart healthcare Smart city Smart grid Multimedia
Fotia et al. (2023)	Edge and IoT architecture and trust	Edge-based IoT architecture Trust need in edge IoT Evaluating trusted edge IoT		✓	✓			✓					Blockchain in edge-IoT Consumption computation Security and reliability Latency and privacy	N/A
Huo et al. (2022)	A blockchain framework in IIoT	Background in IIoT & blockchain Blockchain IIoT pros & cons			✓	✓	✓					✓	Security and privacy Concurrency and throughput Lightweight computation Customized platforms	Supply chain Energy trading Large-scale IoT
Wang et al. (2020)	Blockchain in IIoT and Industry 4.0	Overview of security in IoT IIoT integration of blockchain Blockchain IoT applications											Performance Privacy Increasing complexity Standardized platform	Electric vehicle Smart cities Mobile commerce Trace food source
Wang et al. (2019)	Pros & cons in blockchain-based IoT	Organization of blockchain network Scalability aspect & applications			✓	✓	✓						Lightweight devices Resource demand Mobility affect performance Latency and capacity	N/A
Reyna et al. (2018)	Blockchain-based IoT	Integration of blockchain & IoT Challenges in blockchain IoT Evaluating performance											Capacity and scalability Security & privacy Smart contract Legal issues	Energy trading Identity management Automation Supply chain
Saxena et al. (2021)	Security boosts in blockchain-based IoT	IoT attacks & challenges Various blockchain usages Future directions	✓	✓	✓	✓				✓			Security & privacy Power consumption Capacity and scalability Legislative issues	Supply chain Smart cities VANET Smart healthcare
Dai et al. (2019)	Blockchain & IoT	IoT and its limitations Blockchain overview Convergence of Blockchain IoT Blockchain IoT architecture				✓							Resource constraints Privacy & security Incentive mechanism Scalability Big data analytics	Smart manufacturing Supply chain Smart grid Smart healthcare Internet of vehicles
Xu et al. (2021b)	Blockchain-based IoT	Security and reliability Blockchain IoT types			✓	✓	✓						Performance data processing Suitable consensus Data communication	Healthcare industry Traffic management Smart city
Lone and Naaz (2021)	Blockchain smart contract in IoT	Smart contract securing IoT Issues in IoT smart contract		✓	✓	✓							Evaluation smart contracts Lightweight blockchain	Key management Authentication Data auditing
Wang et al. (2022b)	EI & blockchain	Integration of blockchain & EI Consensus & scalability											Heterogeneous computing Power computation Hardware security Quantization & Trading	Internet of Vehicle Smart healthcare Smart manufacturing Smart grid
Gadekallu et al. (2022)	Blockchain & EoT	Integration of blockchain & EoT Application and notable challenges			✓	✓	✓	✓					Security in blockchain Standardization Resource management Scalability	Smart transport Smart grid Smart city Smart healthcare
Yang et al. (2019)	Blockchain & EoT	Integration of blockchain and edge Frameworks and functionalities Research challenges.		✓		✓	✓			✓			Big data & scalability Privacy and security Self-organization Resource management	Smart homes Smart city Smart healthcare Virtual resources
Ours	Blockchain & edge IoT	Integration of blockchain-based edge IoT Novel 6-layer architecture Blockchain in network paradigm Pros & cons of blockchain deployed types Deep analysis of security requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Distributed AI Sensor–edge deployment 6G usage	Smart grid Smart rescue Smart health

challenges related to application scenarios, performance, task management, and new issues that need to be addressed. While the benefits of decentralization are attractive, it is important to carefully evaluate the trade-offs and limitations before deploying blockchain at the edge and sensor device layers in real-world scenarios.

8.1.4. Coupling blockchain and sensor–edge layer

One potential advantage of deploying blockchain at the edge and sensor device layers is the elimination of the cloud and enhanced decentralization. This reduces the need for trust in a single component and can improve the overall security and reliability of the system. However, this approach also comes with challenges and limitations that must be carefully considered. Managing the diversity of blockchains in a coupling blockchain and sensor–edge–cloud layer can be challenging and may pose issues related to application scenarios, performance, task management, and new problems that require attention. Besides, further examinations and real-world usage cases are also necessary to fully evaluate the benefits and drawbacks of this approach.

In summary, blockchain technology has found diverse applications in computing paradigms, particularly in sensor–edge–cloud systems. However, choosing the right blockchain deployment for a specific use case can be challenging, as no single deployment can satisfy all

Table 4
A summary of current blockchain-empowered edge computing: Architecture, service, domain, platforms.

Study	Blockchain		Blockchain deployment	Security										Application	
	Type[a]	Extra[b]		R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	Service[c]	Domain[d]
Gai et al. (2019)	P	SC	Edge	✓			✓			✓		✓		Resource	Smart grid
Lang et al. (2022)	P	SC	Edge	✓	✓		✓		✓					Resource	VEC
Masuduzzaman et al. (2022)	P	SC	Edge	✓	✓	✓				✓		✓		Resource	Transport
Nguyen et al. (2023a)	P	SC	Edge	✓	✓	✓	✓		✓	✓	✓	✓	✓	Resource	UAV
Yuan et al. (2022)	P	–	Edge		✓				✓	✓				Resource	MEC
Liu et al. (2021)	P	–	Edge		✓			✓	✓		✓	✓	✓	Resource	VEC
Wang et al. (2022a)	–	–	Edge	✓						✓	✓	✓		Resource	MobiCrow
Xu et al. (2021a)	P-less	–	Edge					✓		✓				Resource	UAV
Nguyen et al. (2022)	P	–	Edge		✓	✓	✓		✓	✓	✓	✓	✓	COM	VEC
Nguyen et al. (2019)	P	–	Edge		✓	✓	✓		✓	✓	✓		✓	COM	UAV
Nguyen et al. (2021a)	P-less	–	Edge	✓	✓		✓	✓	✓	✓	✓		✓	AUTH	FL
Yang et al. (2021)	P	SC, Off	Edge							✓			✓	Access	Smart grid
Zhang et al. (2022)	P	SC	Cloud-Edge				✓		✓					Resource	MEC/VANETs
Islam et al. (2021)	P	SC	Cloud-Edge							✓				Resource	VEC
Lu et al. (2022)	P	–	Cloud-Edge		✓						✓	✓		Resource	VEC
Bai et al. (2022)	P	SC, Off	Cloud-Edge	✓					✓	✓	✓	✓	✓	Resource	IIE
Hu et al. (2021)	–	SC, Off	Cloud-Edge	✓	✓					✓		✓	✓	Resource	Supply chain
Guo et al. (2022)	P	SC, Off	Cloud-Edge	✓		✓	✓			✓		✓		KEY	Health
Li et al. (2023)	P-less		Cloud-Edge	✓			✓	✓		✓	✓	✓		KEY	MEC
Yang et al. (2022)	P-less	–	Cloud-Edge							✓				COM	Transport
Awad Abdellatif et al. (2021)	P	–	Cloud-Edge		✓						✓	✓		COM	Health
Baker et al. (2022)	P	SC	Cloud-Edge	✓		✓					✓		✓	AUTH	Transport
Zhang et al. (2021)	–	–	Cloud-Edge						✓			✓		AUTH	IIE
Xu et al. (2022)	P-less	–	Cloud-Edge	✓			✓				✓	✓	✓	AUTH	–
Wang et al. (2021)	P-less	–	Cloud-Edge	✓		✓						✓	✓	AUTH	Health
Li et al. (2021)	P	SC	Cloud-Edge-Sensor						✓			✓		Resource	MEC
Fan et al. (2021)	–	SC	Cloud-Edge-Sensor									✓		Resource	–
Latif et al. (2022)	P	SC, Off	Edge-Sensor							✓		✓		Resource	Smart city
Gumaei et al. (2021)	–	SC	Edge-Sensor	✓			✓							AUTH	UAV
Ming et al. (2022)	–	SC	–	✓		✓				✓	✓	✓		Resource	Health

[a] **Type:** P = Permissioned, P-less = Permissionless.

[b] **Extra:** SC = Smart Contract, Off = Off-chain.

[c] **Service:** Access = Access Control, AUTH= Authentication, COM = Communication, Resource = Resource management, KEY = Key Management.

[d] **Domain:** FL = Federated Learning, IIE = Industrial Internet of Energy, MobiCrow = Mobile Crowdsourcing, VEC = Vehicular Edge Computing.

requirements. The selection of a suitable blockchain deployment should be based on the specific applications and use cases. For example, if the system aims to provide an open platform for collaboration, potential candidates are the full coupling of blockchain and the edge layer and the coupling of blockchain and the sensor–edge layer. On the other hand, if the system requires less powerful computation or support from the cloud for heavy computational tasks, the best options are the coupling of blockchain and the edge–cloud layer and the coupling of blockchain and the sensor–edge–cloud layer.

As an illustration, smart healthcare and smart maritime SaR systems are suitable for the coupling of blockchain and the edge–cloud layer and the coupling of blockchain and the sensor–edge–cloud layer. The blockchain-based ecosystems in these use cases support swift reactions from responsible parties and autonomous operations during urgent emergencies. However, smart grid usage requires collaboration among parties to form a democratic system, such as energy management. Therefore, different blockchain deployments should be considered for different use cases to maximize their potential benefits.

8.2. Security: blockchain-based edge

Although edge computing helps improve the security of blockchain-based IoT systems, it is not ensured that the complete end-to-end IoT system is secured. For instance, resource-constrained devices such as wearable or implantable devices are not equipped with powerful hardware and have limited battery capacity. Therefore, those devices cannot run advanced cryptography algorithms to provide a high level of security. According to The United States Food and Drug Administration, approximately 4000 insulin pumps could be compromised (Voelker, 2019). In order to increase the security levels of these devices, it is necessary to provide some computation capabilities for these devices to run security algorithms such as cryptography. However, when more computations are carried out on devices, more energy will be consumed, and latency also increases. One of the possible solutions dealing with this trade-off is to choose a proper energy-efficient microcontroller or one that is powerful enough to run security algorithms with low latency. Another possible solution is applying security algorithms (Moosavi et al., 2016) that shift computations from sensor devices to edge devices or servers while maintaining end-to-end security. In addition, communication between middle layers, such as edge or fog layers, must be considered. It is noted that the fog layer, in this case, can be the layer between the edge layers and the blockchain. The fog layer is mainly responsible for managing different aspects related to networking, including bandwidth, latency, and communication resources. In many conventional blockchain edge-based systems, communication security is sometimes lack of consideration; for example, data transmitted over the layers or networks are not properly protected.

Table 4 illustrates that current state-of-the-art works on blockchain-based edge IoT cannot fulfill all ten security requirements discussed in Section 5. In general, these works only satisfy 5 to 7 security requirements. While most of them meet confidentiality, trust/confidence, transparency, availability, and automaticity requirements due to the benefits of blockchain, automaticity security cannot be guaranteed. Therefore, enhanced smart contracts should be carefully designed to handle all security issues, including reentrancy attacks, frontrunning, oracle manipulation, timestamp dependence, insecure arithmetic, denial of service, griefing, and force-feeding. A single mistake or issue can result in insecure smart contracts. On the other hand, authentication, authorization, privacy, and tolerance are often neglected in most works, although they can be easily met by applying the approaches discussed in Section 5. It is noted that the number of fulfilled security requirements does not depend on the blockchain type, deployment type, service, or application domain.

Compared with state-of-the-art approaches or architectures, the developed blockchain-based edge IoT system architecture is more enhanced and flexible as it can fulfill all ten security requirements. In our previous work on Internet-of-Drones for SaR (Nguyen et al., 2023a), the authors demonstrated that the proposed blockchain-based edge IoT system architecture helped achieve the goal of fulfilling all ten security requirements. In the discussed blockchain-based edge IoT system architecture for time-critical smart healthcare shown in Section 6, cloud servers are necessary for providing real-time streaming data. In this case, security issues related to cloud servers must be carefully considered to avoid vulnerabilities. For example, streaming data must be permanently deleted after a short period, such as a few minutes. Temporary data on cloud servers must also be protected to prevent unauthorized duplication or modification of the data.

8.3. Potential applications

Section 6 analyzes three main application domains, including smart health monitoring, smart grid, and SaR. However, the developed blockchain-based edge IoT system architecture can also be applied to many other areas, such as IIoT, agriculture, supply chain management, border control, smart cities, and also specific services, including life-cycle management, identity management, and asset tracking.

In environmental monitoring, IoT devices can capture various environmental data, such as air quality, water quality, weather patterns, temperature, humidity, and wind speed. The collected data can undergo preprocessing to remove noise and save bandwidth before being sent to a local edge control station responsible for specific areas. AI-based algorithms can then provide real-time analysis, such as predicting the intensity level of an incoming storm. The analysis results can be added to blocks of a blockchain network, along with the complete data before analysis, if needed. Smart contracts can also be included to provide some level of automation, such as sending necessary medicines to areas affected by a storm.

For time-critical applications, such as emergency response, financial trading, or industrial automation, cloud servers can be used to host temporary streaming data, which can then be remotely monitored in real-time. Private or public cloud servers can be used, depending on the application and network infrastructure. For permissioned blockchains, like Hyperledger Fabric, private cloud servers are preferred as only registered users can monitor the data. In contrast, for permissionless blockchains like Ethereum, any cloud server that meets the system requirements can be used as the current analyses from Nguyen et al. (2023b).

Addressing concerns related to data quality and non-repudiation, a blockchain-driven edge system emerges as a compelling solution to safeguard the integrity of data throughout its entire lifecycle—from its collection and processing to storage. In practical applications such as big data management, including scenarios like smart city implementations and supply chain management, product quality assurance is intricately linked to the operations surrounding those products. Here, blockchain technology comes into play by not only ensuring data quality but also bolstering non-repudiation measures, solidifying its position as a vital component in guaranteeing product quality and data trustworthiness.

Blockchain's primary advantage lies in fostering transparency and interoperability. Its fundamental idea of decentralization makes it a key component in the creation of an international protocol, which facilitates effortless communication and data exchange across various participants and services. Such an approach is particularly beneficial in the diverse and fragmented landscape of heterogeneous edge–cloud computing and networks, where seamless integration is crucial.

In all these applications, the developed blockchain-based edge IoT system architecture provides a time series database with many benefits, such as security, transparency, trust, and availability, which can help overcome the limitations of traditional IoT systems. These characteristics establish the system as a foundational element for numerous security services, as detailed in Section 4.3 and Section 8.2. These services are crucial across various application domains, as outlined in Table 4. Examples include decentralized data management, the use of smart contracts for automating services, efficient supply chain management, and the integration of distributed AI and machine learning techniques.

9. Opportunities and open directions

The fusion of edge computing and blockchain within IoT research presents a landscape rife with both challenges and opportunities. Accordingly, this section delineates future research directions guided by specific Research Questions (RQs).

RQ 1: *How can hetero-blockchain networks be optimized in edge computing to balance security, privacy, and performance, while facilitating secure data and resource sharing?*

Expanding on the idea of extending blockchain-based edge systems to serve an ecosystem, the use of hetero-blockchain networks can bring several advantages. Different applications have varying security, privacy, and performance requirements, so utilizing a single blockchain network may not be feasible. Hetero-blockchain networks allow each application to use the appropriate blockchain types that meet its specific requirements. Moreover, these hetero-blockchain networks can intersect with other blockchain networks of other applications, enabling secure and efficient sharing of data and resources. This research question aims to investigate the challenges and strategies involved in deploying and managing hetero-blockchain networks within edge computing environments. It focuses on understanding how different blockchain types can be effectively integrated to meet the varying needs of different applications, and how these networks can interact with each other to facilitate data and resource sharing. The question also opens up avenues for exploring architectural designs, governance models, and interoperability standards that could support such a complex, multi-blockchain environment.

RQ 2: *How does integrating blockchain at the sensor–edge layer affect decentralization and data processing efficiency in distributed systems?*

The coupling of blockchain on the sensor–edge layer from Section 4 can bring significant benefits to the performance and decentralization of the system. Via integrating blockchain technology on the sensor–edge layer, data can be stored and processed locally, reducing the need for communication. Although the potential benefits of the coupling of blockchain on the sensor–edge layer have been recognized, recent studies lack consideration of this architecture. Therefore, further research is needed to explore the implementation of blockchain technology on the sensor–edge layer and the potential benefits it can bring to the system. This research question aims to investigate the specific effects of incorporating blockchain technology at the sensor–edge layer of distributed systems. It seeks to understand both the theoretical and practical aspects of this integration, focusing on the potential improvements in system performance, efficiency in local data processing, and the degree of decentralization achieved. The question also invites exploration into the challenges and best practices for implementing such an architecture, considering the current gap in existing studies.

RQ 3: *How can blockchain enhance trustworthiness, including data security and authentication, when integrated with 6G in edge computing networks?*

Integrating advanced wireless communication technologies, such as 6G, with blockchain-based edge systems can improve service quality by reducing latency and enhancing reliability. However, upgrading edge computing and network infrastructures for efficiency using 6G is necessary (Nguyen et al., 2021c). The het-cloud architecture proposed by Ziegler et al. (2021) presents trustworthiness challenges due to its distributed and heterogeneous nature, which includes edge, private, central, and public clouds. The scale of millions of subnetworks and billions of data sources, such as sensors, further complicates these challenges. To address these issues, multivendor trust domains must connect untrusted domains as subnetworks of data generation via the cloud stack and topologies. The data generation side threatens trust data collection, while the network side requires secure definitions, such as authentication and identity, to ensure trust in subnetworks. While reputation is frequently the basis of trust formation, novel technologies can shape trust in the era of advanced technologies. Prior works of technology (Ylianttila et al., 2020) and Nguyen et al. (2021c) are promising solutions in leveraging blockchain for trust formation in the 6G era, particularly when applied to EI. Beyond the foregoing, blockchain technology can also enable collaboration between service providers to achieve the required trust (Nguyen et al., 2022, 2019). Finally, the immutability and transparency of blockchain support auditing by keeping track of records to build trust in communication and

verification, making it an ideal solution for ensuring trust in advanced wireless communication systems. This question aims to explore the role of blockchain in addressing trust and security challenges in complex edge computing environments enhanced by 6G technology. It focuses on understanding how blockchain's inherent features like immutability and transparency can contribute to building trust in these systems, especially in the context of multivendor trust domains, secure data collection, and reliable network communication. The question also invites an investigation into the practical aspects of implementing blockchain in such environments, considering the scale and diversity of data sources and network architectures.

RQ 4: *How can blockchain-based edge systems improve AI tool functionality and reliability in low-connectivity environments, and ensure real-time accuracy of their outputs?*

ChatGPT, a chatbot developed by OpenAI and enhanced with supervised and reinforcement learning techniques, is a widely used tool in various fields and applications. By reducing workload and improving efficiency, ChatGPT offers many advantages. However, it requires internet access and a suitable browser to function, which can pose challenges in areas with unstable or no internet connectivity. To overcome these challenges while maintaining high-quality service, the combination of 6G, ChatGPT, and a blockchain-based edge system can be utilized. Customized GPT-3-powered language tools can be applied at edge devices to provide additional value and perform actions. However, before utilizing the information provided by AI tools such as GPT-3-powered language tools, it is necessary to validate the accuracy of the information. This question aims to explore the potential of combining advanced technologies like 6G and blockchain with AI-driven tools in edge computing environments, for example, Large Language Model (LLM) multi-agent negotiation or synergizing LLMs. The focus is on how these integrations can mitigate connectivity challenges and improve service quality. Particularly, Han et al. (2024), Gong (2023), Luo et al. (2023) underscore the usage of blockchain technology to foster collaborative AI formation, especially interconnecting LLMs. Additionally, the question addresses the critical aspect of ensuring the reliability and accuracy of the information provided by AI tools, which is essential for their practical application in various fields.

RQ 5: *How can 6G and blockchain integration with advanced communication technologies improve resource management and coordination in edge computing's distributed intelligence systems, and optimize resource selection and utilization?*

To support the trend of distributed intelligence in edge computing, it is essential to equip blockchain-based edge IoT with mechanisms or tools for monitoring edge resources. Coordinators should also be developed to select suitable edge devices or resources based on the results obtained from resource monitoring. Utilizing blockchain is crucial to enable security, fairness, and decentralization in distributed systems. One emerging development direction is decentralized marketplaces for edge resources, where edge devices can autonomously trade computational power, storage, and data through a blockchain-based platform. The exploration of smart contracts within blockchain frameworks offers a promising avenue for automating the orchestration of edge computing resources. Smart contracts can enforce predefined rules for data sharing and processing among participating nodes, thereby simplifying the governance of distributed intelligence applications. This automation is particularly beneficial in scenarios involving large-scale IoT deployments, where manual coordination is impractical. Recently, blockchain technology has become the prime solution for collaboration among parties in computation aspects, including cloud, fog, edge, and mist computing. As edge devices often operate in unsecured environments, the application of blockchain can introduce decentralized security mechanisms that protect against tampering and eavesdropping. For instance, blockchain can be used to create immutable logs of edge device activities, enabling the detection and tracing of malicious actions. Additionally, with the development of advanced communication technologies like 6G and Wi-Fi, the extension of edge computing, especially distributed intelligence, is the next evolution after the success of this computing layer. These advanced communication technologies promise to deliver higher bandwidth and lower latency, which are crucial for supporting real-time analytics and decision-making in distributed intelligence frameworks. With the privacy-preserving capabilities of federated learning, this blockchain-based system not only facilitates sharing model updates without disclosing the raw data but also establishes a secure and transparent environment. It enables the detection and tracing of adversary attacks, ensuring the integrity of global model parameters against malicious client interventions. Therefore, key directions for success include studying resource management, collaboration among heterogeneous networks, and scheduling management. It is important to develop these areas to enable the use of distributed intelligence in edge computing and unlock its full potential. This research question aims to investigate the role of blockchain technology in supporting distributed intelligence in edge computing, particularly focusing on resource monitoring and coordination. It explores how blockchain, in conjunction with emerging communication technologies like 6G and Wi-Fi, can facilitate secure, fair, and efficient management of edge resources. The question also addresses the need for developing novel and particular mechanisms or tools to select and utilize edge devices and resources effectively, which is crucial for the advancement of distributed intelligence in edge computing environments.

RQ 6: *How can AI, particularly reinforcement learning, be effectively utilized to achieve optimal self-configuration and auto-configuration in edge computing and blockchain-integrated IoT systems?*

Reinforcement learning plays a pivotal role in enabling self-configuration and auto-configuration, particularly in the integration of edge computing and blockchain within IoT frameworks. The dynamic nature of networks, both heterogeneous and homogeneous, and their inherent flexibility in participation, necessitate a robust autonomous configuration mechanism. This is where the significance of reinforcement learning becomes apparent, as evidenced by advanced applications like ChatGPT. By integrating AI into the system's configuration process, we open a promising avenue for research. The goal is to achieve optimal self-configuration and auto-configuration, especially critical in emergencies or response to system changes such as crashes and failures in computation, communication, and storage. This question aims to explore the application of reinforcement learning in the context of integrating edge computing and blockchain within IoT frameworks. It focuses on understanding how reinforcement learning can facilitate robust and efficient autonomous configuration mechanisms, especially in challenging scenarios like network changes, emergencies, and system failures. The question also invites investigation into the potential of AI-driven approaches to enhance system resilience and adaptability in heterogeneous and dynamic network environments.

10. Conclusion

While IoT systems have found numerous applications, they still face challenges such as security vulnerabilities, unreliability, and high latency. To address these limitations, the integration of edge computing and blockchain has been proposed. However, a comprehensive review of these technologies' combined use in IoT systems is lacking. This paper aims to fill this gap by providing a thorough analysis of blockchain-based edge systems, where edge computing and blockchain work together to improve IoT systems' performance and security. The review includes an in-depth analysis of the security requirements that these systems must meet, such as confidentiality, integrity, authentication, authorization/access control, privacy, trust/confidence, transparency, availability, secure automaticity, and tolerance. The paper also provides an overview and evaluation of blockchain-based edge systems based on these requirements. Moreover, the paper discusses and analyzes the blockchain-based edge systems' suitability for various

applications, such as smart healthcare, smart grid, and SaR. Finally, the paper highlights different aspects of blockchain-based edge system architectures, including open research questions and future directions in this field.

CRediT authorship contribution statement

Tri Nguyen: Writing – review & editing, Writing – original draft, Visualization, Supervision, Project administration, Methodology, Formal analysis, Conceptualization. **Huong Nguyen:** Validation, Methodology, Visualization, Writing – original draft, Writing – review & editing. **Tuan Nguyen Gia:** Conceptualization, Formal analysis, Validation, Writing – original draft.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Tri Nguyen, Huong Nguyen reports financial support was provided by Academy of Finland. Huong Nguyen reports financial support was provided by Business Finland. Tri Nguyen, Huong Nguyen reports financial support was provided by Horizon Europe. Tri Nguyen reports a relationship with University of Oulu Infotech Oulu that includes: funding grants.

Data availability

No data was used for the research described in the article.

Acknowledgments

This research is supported by the Research Council of Finland, 6G Flagship (grant 346208), the FRACTAL ECSEL JU (grant 877056), funded by Horizon Europe, and Business Finland with the Neural pub/sub (8754/31/2022) and Enabling Metaverse (EMETA) (8719/31/2022).

References

Abbas, N., Zhang, Y., Taherkordi, A., Skeie, T., 2017. Mobile edge computing: A survey. IEEE Internet Things J. 5 (1), 450–465.

Aldowah, H., Ul Rehman, S., Umar, I., 2021. Trust in IoT systems: a vision on the current issues, challenges, and recommended solutions. Adv. Smart Soft Comput. 329–339.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al., 2018. Hyperledger fabric: A distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference. EuroSys '18, Association for Computing Machinery, New York, NY, USA, http://dx.doi.org/10.1145/3190508.3190538.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., et al., 2010. A view of cloud computing. Commun. ACM 53 (4), 50–58. http://dx.doi.org/10.1145/1721654.1721672, URL: http://doi.acm.org/10.1145/1721654.1721672.

Awad Abdellatif, A., Samara, L., Mohamed, A., Erbad, A., Chiasserini, C.F., Guizani, M., O'Connor, M.D., Laughton, J., 2021. MEdge-Chain: Leveraging edge computing and blockchain for efficient medical data exchange. IEEE Internet Things J. 8 (21), 15762–15775. http://dx.doi.org/10.1109/JIOT.2021.3052910.

Bai, F., Shen, T., Yu, Z., Zeng, K., Gong, B., 2022. Trustworthy blockchain-empowered collaborative edge computing-as-a-service scheduling and data sharing in the IIoE. IEEE Internet Things J. 9 (16), 14752–14766. http://dx.doi.org/10.1109/JIOT.2021.3058125.

Baker, T., Asim, M., Samwini, H., Shamim, N., Alani, M.M., Buyya, R., 2022. A blockchain-based fog-oriented lightweight framework for smart public vehicular transportation systems. Comput. Netw. 203, 108676. http://dx.doi.org/10.1016/j.comnet.2021.108676, URL: https://www.sciencedirect.com/science/article/pii/S138912862100548X.

Belotti, M., Božić, N., Pujolle, G., Secci, S., 2019. A vademecum on blockchain technologies: When, Which, and How. IEEE Commun. Surv. Tutor. 21 (4), 3796–3838. http://dx.doi.org/10.1109/COMST.2019.2928178.

Bertino, E., Kundu, A., Sura, Z., 2019. Data transparency with blockchain and AI ethics. J. Data Inf. Qual. (JDIQ) 11 (4), 1–8.

Bonomi, F., Milito, R., Zhu, J., Addepalli, S., 2012. Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. MCC '12, Association for Computing Machinery, New York, NY, USA, pp. 13–16. http://dx.doi.org/10.1145/2342509.2342513.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., Sirdey, R., 2017. Towards better availability and accountability for IoT updates by means of a blockchain. In: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 50–58. http://dx.doi.org/10.1109/EuroSPW.2017.50.

Buterin, V., 2014. A next-generation smart contract and decentralized application platform. 3, (37), white paper.

Chainlink, 2023. Connecting the world to blockchains. https://chain.link/. (Accessed 27 February 2023).

Chen, Y., Li, H., Li, K., Zhang, J., 2017. An improved P2P file system scheme based on IPFS and blockchain. In: 2017 IEEE International Conference on Big Data (Big Data). pp. 2652–2657. http://dx.doi.org/10.1109/BigData.2017.8258226.

Dai, H.-N., Zheng, Z., Zhang, Y., 2019. Blockchain for internet of things: A survey. IEEE Internet Things J. 6 (5), 8076–8094. http://dx.doi.org/10.1109/JIOT.2019.2920987.

De Filippi, P., Mannan, M., Reijers, W., 2020. Blockchain as a confidence machine: The problem of trust & challenges of governance. Technol. Soc. 62, 101284.

Dolui, K., Datta, S.K., 2017. Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. In: 2017 Global Internet of Things Summit. GIoTS, IEEE, pp. 1–6.

Dunphy, P., Petitcolas, F.A., 2018. A first look at identity management schemes on the blockchain. IEEE Secur. Priv. 16 (4), 20–29. http://dx.doi.org/10.1109/MSP.2018.3111247.

Fan, Y., Wang, L., Wu, W., Du, D., 2021. Cloud/edge computing resource allocation and pricing for mobile blockchain: An iterative greedy and search approach. IEEE Trans. Comput. Soc. Syst. 8 (2), http://dx.doi.org/10.1109/TCSS.2021.3049152.

Fazeldehkordi, E., Grønli, T.M., 2022. A survey of security architectures for edge computing-based IoT. IoT 3 (3), 332–365.

Feng, J., Richard Yu, F., Pei, Q., Chu, X., Du, J., Zhu, L., 2020. Cooperative computation offloading and resource allocation for blockchain-enabled mobile-edge computing: A deep reinforcement learning approach. IEEE Internet Things J. 7 (7), 6214–6228. http://dx.doi.org/10.1109/JIOT.2019.2961707.

Fetahu, L., Maraj, A., Havolli, A., 2022. Internet of things (IoT) benefits, future perspective, and implementation challenges. In: 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology. MIPRO, pp. 399–404. http://dx.doi.org/10.23919/MIPRO55190.2022.9803487.

Firouzi, F., Farahani, B., Marinšek, A., 2022. The convergence and interplay of edge, fog, and cloud in the AI-driven internet of things (IoT). Inf. Syst. 107, 101840. http://dx.doi.org/10.1016/j.is.2021.101840, URL: https://www.sciencedirect.com/science/article/pii/S0306437921000776.

Fotia, L., Delicato, F., Fortino, G., 2023. Trust in edge-based internet of things architectures: State of the art and research challenges. ACM Comput. Surv. 55 (9), http://dx.doi.org/10.1145/3558779, https://doi.org/10.1145/3558779.

Gadekallu, T.R., Pham, Q.V., Nguyen, D.C., Maddikunta, P.K.R., Deepa, N., Prabadevi, B., Pathirana, P.N., Zhao, J., Hwang, W.J., 2022. Blockchain for edge of things: Applications, opportunities, and challenges. IEEE Internet Things J. 9 (2), 964–988. http://dx.doi.org/10.1109/JIOT.2021.3119639.

Gai, K., Wu, Y., Zhu, L., Xu, L., Zhang, Y., 2019. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet Things J. 6 (5), 7992–8004. http://dx.doi.org/10.1109/JIOT.2019.2904303.

General Medical Council, 2017. Confidentiality: good practice in handling patient information. Accessed 28 October 2022.

Gia, T.N., Jiang, M., Rahmani, A.M., Westerlund, T., Liljeberg, P., Tenhunen, H., 2015. Fog computing in healthcare internet of things: A case study on ECG feature extraction. In: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. pp. 356–363. http://dx.doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.51.

Gia, T.N., Qingqing, L., Queralta, J.P., Zou, Z., Tenhunen, H., Westerlund, T., 2019. Edge AI in smart farming IoT: CNNs at the edge and fog computing with LoRa. In: 2019 IEEE AFRICON. pp. 1–6. http://dx.doi.org/10.1109/AFRICON46755.2019.9134049.

Gia, T.N., Thanigaivelan, N.K., Rahmani, A.M., Westerlund, T., Liljeberg, P., Tenhunen, H., 2014. Customizing 6lowpan networks towards internet-of-things based ubiquitous healthcare systems. In: 2014 NORCHIP. pp. 1–6. http://dx.doi.org/10.1109/NORCHIP.2014.7004716.

Gong, Y., 2023. Dynamic large language models on blockchains. arXiv:2307.10549.

Gumaei, A., Al-Rakhami, M., Hassan, M.M., Pace, P., Alai, G., Lin, K., Fortino, G., 2021. Deep learning and blockchain with edge computing for 5G-enabled drone identification and flight mode detection. IEEE Network 35 (1), 94–100. http://dx.doi.org/10.1109/MNET.011.2000204.

Guo, H., Li, W., Nejad, M., Shen, C.C., 2022. A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms. IEEE Trans. Netw. Serv. Manag. 1. http://dx.doi.org/10.1109/TNSM.2022.3186006.

Han, R., Yan, Z., Liang, X., Yang, L.T., 2022. How can incentive mechanisms and blockchain benefit with each other? A survey. 55 (7), http://dx.doi.org/10.1145/3539604.

Han, S., Zhang, Q., Yao, Y., Jin, W., Xu, Z., He, C., 2024. LLM multi-agent systems: Challenges and open problems. arXiv:2402.03578.

Hasan, O., Brunie, L., Bertino, E., 2022. Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey. ACM Comput. Surv. 55 (2), http://dx.doi.org/10.1145/3490236.

Hu, S., Huang, S., Huang, J., Su, J., 2021. Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis. Comput. Ind. Eng. 153, 107079. http://dx.doi.org/10.1016/j.cie.2020.107079, URL: https://www.sciencedirect.com/science/article/pii/S036083522030749X.

Hu, Y.C., Patel, M., Sabella, D., Sprecher, N., Young, V., 2015. Mobile edge computing—A key technology towards 5G. ETSI White Paper 11 (11), 1–16.

Huo, R., Zeng, S., Wang, Z., Shang, J., Chen, W., Huang, T., Wang, S., Yu, F.R., Liu, Y., 2022. A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges. IEEE Commun. Surv. Tutor. 24 (1), 88–122. http://dx.doi.org/10.1109/COMST.2022.3141490.

Ion, M., Danzi, A., Koshutanski, H., Telesca, L., 2008. A peer-to-peer multidimensional trust model for digital ecosystems. In: 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies. IEEE, pp. 461–469.

Islam, S., Badsha, S., Sengupta, S., La, H., Khalil, I., Atiquzzaman, M., 2021. Blockchain-enabled intelligent vehicular edge computing. IEEE Network 35 (3), 125–131. http://dx.doi.org/10.1109/MNET.011.2000554.

Jadeja, Y., Modi, K., 2012. Cloud computing-concepts, architecture and challenges. In: 2012 International Conference on Computing, Electronics and Electrical Technologies. ICCEET, IEEE, pp. 877–880.

Khan, H., Masood, T., 2022. Impact of blockchain technology on smart grids. Energies 15 (19), 7189.

Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., Zeng, P., Khan, M., Das, S.K., 2022. Edge-computing-driven internet of things: A survey. ACM Comput. Surv. http://dx.doi.org/10.1145/3555308.

Lang, P., Tian, D., Duan, X., Zhou, J., Sheng, Z., Leung, V.C.M., 2022. Cooperative computation offloading in blockchain-based vehicular edge computing networks. IEEE Trans. Intell. Veh. 7 (3), 783–798. http://dx.doi.org/10.1109/TIV.2022.3190308.

Laroui, M., Nour, B., Moungla, H., Cherif, M.A., Afifi, H., Guizani, M., 2021. Edge and fog computing for IoT: A survey on current research activities & future directions. Comput. Commun. 180, 210–231. http://dx.doi.org/10.1016/j.comcom.2021.09.003, URL: https://www.sciencedirect.com/science/article/pii/S0140366421003327.

Latif, Z., Lee, C., Sharif, K., Helal, S., 2022. SDBlockEdge: SDN-blockchain enabled multihop task offloading in collaborative edge computing. IEEE Sens. J. 22 (15), 15537–15548. http://dx.doi.org/10.1109/JSEN.2022.3184689.

Lee, C.K.M., Huo, Y.Z., Zhang, S.Z., Ng, K.K.H., 2020. Design of a smart manufacturing system with the application of multi-access edge computing and blockchain technology. IEEE Access 8, 28659–28667. http://dx.doi.org/10.1109/ACCESS.2020.2972284.

Li, G., Ren, X., Wu, J., Ji, W., Yu, H., Cao, J., Wang, R., 2021. Blockchain-based mobile edge computing system. Inform. Sci. 561, 70–80. http://dx.doi.org/10.1016/j.ins.2021.01.050, URL: https://www.sciencedirect.com/science/article/pii/S0020025521000888.

Li, J., Wu, J., Chen, L., Li, J., Lam, S.K., 2023. Blockchain-based secure key management for mobile edge computing. IEEE Trans. Mob. Comput. 22 (1), 100–114. http://dx.doi.org/10.1109/TMC.2021.3068717.

Lin, X., Wu, J., Mumtaz, S., Garg, S., Li, J., Guizani, M., 2021. Blockchain-based on-demand computing resource trading in IoV-Assisted smart city. IEEE Trans. Emerg. Top. Comput. 9 (3), 1373–1385. http://dx.doi.org/10.1109/TETC.2020.2971831.

Liu, H., Zhang, S., Zhang, P., Zhou, X., Shao, X., Pu, G., Zhang, Y., 2021. Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. IEEE Trans. Veh. Technol. 70 (6), 6073–6084. http://dx.doi.org/10.1109/TVT.2021.3076780.

Lone, A.H., Naaz, R., 2021. Applicability of blockchain smart contracts in securing internet and IoT: A systematic literature review. Comp. Sci. Rev. 39, 100360. http://dx.doi.org/10.1016/j.cosrev.2020.100360, URL: https://www.sciencedirect.com/science/article/pii/S1574013720304603.

Lu, Y., Zhang, J., Qi, Y., Qi, S., Zheng, Y., Liu, Y., Song, H., Wei, W., 2022. Accelerating at the edge: A storage-elastic blockchain for latency-sensitive vehicular edge computing. IEEE Trans. Intell. Transp. Syst. 23 (8), http://dx.doi.org/10.1109/TITS.2021.3108052.

Luo, H., Luo, J., Vasilakos, A.V., 2023. BC4LLM: Trusted artificial intelligence when blockchain meets large language models. arXiv:2310.06278.

Mahmud, R., Kotagiri, R., Buyya, R., 2018. Fog computing: A taxonomy, survey and future directions. In: Internet of Everything. Springer, pp. 103–130.

Mao, Y., You, C., Zhang, J., Huang, K., Letaief, K.B., 2017. A survey on mobile edge computing: The communication perspective. IEEE Commun. Surv. Tutorials 19 (4), 2322–2358. http://dx.doi.org/10.1109/COMST.2017.2745201.

Masuduzzaman, M., Islam, A., Sadia, K., Shin, S.Y., 2022. UAV-based MEC-assisted automated traffic management scheme using blockchain. Future Gener. Comput. Syst. 134, 256–270. http://dx.doi.org/10.1016/j.future.2022.04.018, URL: https://www.sciencedirect.com/science/article/pii/S0167739X22001418.

Merkle, R.C., 1987. A digital signature based on a conventional encryption function. In: Conference on the Theory and Application of Cryptographic Techniques. Springer, pp. 369–378.

Metwaly, A., Queralta, J.P., Sarker, V.K., Gia, T.N., Nasir, O., Westerlund, T., 2019. Edge computing with embedded ai: Thermal image analysis for occupancy estimation in intelligent buildings. In: Proceedings of the INTelligent Embedded Systems Architectures and Applications Workshop 2019. pp. 1–6.

Ming, Z., Zhou, M., Cui, L., Yang, S., 2022. FAITH: A fast blockchain-assisted edge computing platform for healthcare applications. IEEE Trans. Ind. Inform. 18 (12), 9217–9226. http://dx.doi.org/10.1109/TII.2022.3166813.

Moosavi, S.R., Gia, T.N., Nigussie, E., Rahmani, A.M., Virtanen, S., Tenhunen, H., Isoaho, J., 2016. End-to-end security scheme for mobility enabled healthcare internet of things. Future Gener. Comput. Syst. 64, 108–124. http://dx.doi.org/10.1016/j.future.2016.02.020.

Moosavi, S.R., Gia, T.N., Rahmani, A.M., Nigussie, E., Virtanen, S., Isoaho, J., Tenhunen, H., 2015. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Comput. Sci. 52, 452–459. http://dx.doi.org/10.1016/j.procs.2015.05.013, URL: https://www.sciencedirect.com/science/article/pii/S1877050915008133, The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015).

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus. Rev. 21260.

Nawaz, A., Queralta, J.P., Guan, J., Awais, M., Gia, T.N., Bashir, A.K., Kan, H., Westerlund, T., 2020. Edge computing to secure iot data ownership and trade with the ethereum blockchain. Sensors 20 (14), 3965.

Nguyen, D.C., Ding, M., Pham, Q.V., Pathirana, P.N., Le, L.B., Seneviratne, A., Li, J., Niyato, D., Poor, H.V., 2021a. Federated learning meets blockchain in edge computing: Opportunities and challenges. IEEE Internet Things J. 8 (16), 12806–12825. http://dx.doi.org/10.1109/JIOT.2021.3072611.

Nguyen, T., Katila, R., Gia, T.N., 2021b. A novel internet-of-drones and blockchain-based system architecture for search and rescue. In: 2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems. MASS, IEEE, pp. 278–288.

Nguyen, T., Katila, R., Gia, T.N., 2023a. An advanced internet-of-drones system with blockchain for improving quality of service of search and rescue: A feasibility study. Future Gener. Comput. Syst. 140, 36–52.

Nguyen, T., Lovén, L., Partala, J., Pirttikangas, S., 2021c. The intersection of blockchain and 6G technologies. In: 6G Mobile Wireless Networks. Springer International Publishing, Cham, pp. 393–417. http://dx.doi.org/10.1007/978-3-030-72777-2_18.

Nguyen, H., Nguyen, T., Leppänen, T., Partala, J., Pirttikangas, S., 2022. Situation awareness for autonomous vehicles using blockchain-based service cooperation. In: Advanced Information Systems Engineering. Springer International Publishing, Cham, pp. 501–516.

Nguyen, T., Nguyen, H., Partala, J., Pirttikangas, S., 2023b. Trustedmaas: Transforming trust and transparency mobility-as-a-service with blockchain. Future Gener. Comput. Syst. 149, 606–621. http://dx.doi.org/10.1016/j.future.2023.08.011.

Nguyen, T.H., Partala, J., Pirttikangas, S., 2019. Blockchain-based mobility-as-a-service. In: 2019 28th International Conference on Computer Communication and Networks. ICCCN, pp. 1–6. http://dx.doi.org/10.1109/ICCCN.2019.8847027.

Nguyen Gia, T., Jiang, M., Sarker, V.K., Rahmani, A.M., Westerlund, T., Liljeberg, P., Tenhunen, H., 2017. Low-cost fog-assisted health-care IoT system with energy-efficient sensor nodes. In: 2017 13th International Wireless Communications and Mobile Computing Conference. IWCMC, pp. 1765–1770. http://dx.doi.org/10.1109/IWCMC.2017.7986551.

Nguyen Gia, T., Nawaz, A., Peña Querata, J., Tenhunen, H., Westerlund, T., 2020. Artificial intelligence at the edge in the blockchain of things. In: Wireless Mobile Communication and Healthcare: 8th EAI International Conference, MobiHealth 2019, Dublin, Ireland, November 14-15, 2019, Proceedings 8. Springer, pp. 267–280.

Omoniwa, B., Hussain, R., Javed, M.A., Bouk, S.H., Malik, S.A., 2019. Fog/edge computing-based IoT (fecIoT): Architecture, applications, and research issues. IEEE Internet Things J. 6 (3), 4118–4149. http://dx.doi.org/10.1109/JIOT.2018.2875544.

Openzeppelin, 2023. The standard for secure blockchain applications. https://www.openzeppelin.com/. (Accessed 27 February 2023).

Pan, Y., Thulasiraman, P., Wang, Y., 2018. Overview of cloudlet, fog computing, edge computing, and dew computing. In: Proceedings of the 3rd International Workshop on Dew Computing. pp. 20–23.

Peltonen, E., Ahmad, I., Aral, A., Capobianco, M., Ding, A.Y., Gil-Castiñeira, F., Gilman, E., Harjula, E., Jurmu, M., Karvonen, T., Kelanti, M., Leppänen, T., Lovén, L., Mikkonen, T., Mohan, N., Nurmi, P., Pirttikangas, S., Sroka, P., Tarkoma, S., Yang, T., 2022. The many faces of edge intelligence. IEEE Access 10, 104769–104782. http://dx.doi.org/10.1109/ACCESS.2022.3210584.

Qingqing, L., Taipalmaa, J., Queralta, J.P., Gia, T.N., Gabbouj, M., Tenhunen, H., Raitoharju, J., Westerlund, T., 2020. Towards active vision with UAVs in marine search and rescue: Analyzing human detection at variable altitudes. In: 2020 IEEE International Symposium on Safety, Security, and Rescue Robotics. SSRR, IEEE, pp. 65–70.

Queralta, J.P., Gia, T.N., Tenhunen, H., Westerlund, T., 2019. Edge-AI in lora-based health monitoring: Fall detection system with fog computing and LSTM recurrent neural networks. In: 2019 42nd International Conference on Telecommunications and Signal Processing. TSP, pp. 601–604. http://dx.doi.org/10.1109/TSP.2019.8768883.

Ray, P.P., Dash, D., De, D., 2019. Edge computing for internet of things: A survey, e-healthcare case study and future direction. J. Netw. Comput. Appl. 140, 1–22.
Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 88, 173–190. http://dx.doi.org/10.1016/j.future.2018.05.046, URL: https://www.sciencedirect.com/science/article/pii/S0167739X17329205.
Sarker, V.K., Queralta, J.P., Gia, T.N., Tenhunen, H., Westerlund, T., 2019. A survey on LoRa for IoT: Integrating edge computing. In: 2019 Fourth International Conference on Fog and Mobile Edge Computing. FMEC, pp. 295–300. http://dx.doi.org/10.1109/FMEC.2019.8795313.
Satyanarayanan, M., 2017. The emergence of edge computing. Computer 50 (1), 30–39. http://dx.doi.org/10.1109/MC.2017.9.
Satyanarayanan, M., Bahl, P., Cáceres, R., Davies, N., 2009. The case for VM-based cloudlets in mobile computing. IEEE Pervasive Comput. 8 (4), 14–23. http://dx.doi.org/10.1109/MPRV.2009.82.
Saxena, S., Bhushan, B., Ahad, M.A., 2021. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. J. Netw. Comput. Appl. 181, http://dx.doi.org/10.1016/j.jnca.2021.103050, URL: https://www.sciencedirect.com/science/article/pii/S1084804521000758.
Schaub, A., Bazin, R., Hasan, O., Brunie, L., 2016. A trustless privacy-preserving reputation system. In: ICT Systems Security and Privacy Protection. Springer International Publishing, Cham, pp. 398–411.
Sharples, M., Domingue, J., 2016. The blockchain and kudos: A distributed system for educational record, reputation and reward. In: Adaptive and Adaptable Learning. Springer International Publishing, Cham, pp. 490–496.
Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L., 2016. Edge computing: Vision and challenges. IEEE Internet Things J. 3 (5), 637–646. http://dx.doi.org/10.1109/JIOT.2016.2579198.
Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S., et al., 2010. Vision and challenges for realising the internet of things. Clust. Eur. Res. Proj. Internet Things, Eur. Commision 3 (3), 34–36.
Talebkhah, M., Sali, A., Marjani, M., Gordan, M., Hashim, S.J., Rokhani, F.Z., 2021. Iot and big data applications in smart cities: Recent advances, challenges, and critical issues. IEEE Access 9, 55465–55484. http://dx.doi.org/10.1109/ACCESS.2021.3070905.
Tellor, 2023. A decentralized oracle protocol. https://tellor.io/. (Accessed 27 February 2023).
Tian, F., 2016. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: 2016 13th International Conference on Service Systems and Service Management. ICSSSM, pp. 1–6. http://dx.doi.org/10.1109/ICSSSM.2016.7538424.
Tobin, A., Reed, D., 2016. The inevitable rise of self-sovereign identity. Sovrin Found. 29 (2016), 18.
Voelker, R., 2019. Insulin pumps could be hacked. JAMA 322 (5), 393.
Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., Kim, D.I., 2019. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access 7, 22328–22370. http://dx.doi.org/10.1109/ACCESS.2019.2896108.
Wang, W., Huang, H., Xue, L., Li, Q., Malekian, R., Zhang, Y., 2021. Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment. J. Syst. Archit. 115, 102024. http://dx.doi.org/10.1016/j.sysarc.2021.102024, URL: https://www.sciencedirect.com/science/article/pii/S1383762121000333.
Wang, X., Ren, X., Qiu, C., Xiong, Z., Yao, H., Leung, V.C., 2022b. Integrating edge intelligence and blockchain: What, Why, and How. IEEE Commun. Surv. Tutor. 24 (4), 2193–2229. http://dx.doi.org/10.1109/COMST.2022.3189962.
Wang, W., Wang, Y., Duan, P., Liu, T., Tong, X., Cai, Z., 2022a. A triple real-time trajectory privacy protection mechanism based on edge computing and blockchain in mobile crowdsourcing. IEEE Trans. Mob. Comput. 1–18. http://dx.doi.org/10.1109/TMC.2022.3187047.
Wang, Q., Zhu, X., Ni, Y., Gu, L., Zhu, H., 2020. Blockchain for the IoT and industrial IoT: A review. Internet Things 10, 100081. http://dx.doi.org/10.1016/j.iot.2019.100081, URL: https://www.sciencedirect.com/science/article/pii/S254266051930085X, Special Issue of the Elsevier IoT Journal on Blockchain Applications in IoT Environments.
Witnet, 2023. Unleash the real power of smart contracts. https://witnet.io/. (Accessed 27 February 2023).
Wood, G., et al., 2014. Ethereum: A secure decentralised generalised transaction ledger. 151, (2014), pp. 1–32, Ethereum project yellow paper.
Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., Lv, W., 2019. Edge computing security: State of the art and challenges. Proc. IEEE 107 (8), 1608–1631. http://dx.doi.org/10.1109/JPROC.2019.2918437.
Xu, G., Dong, J., Ma, C., Liu, J., Omar Cliff, U.G., 2022. A certificateless signcryption mechanism based on blockchain for edge computing. IEEE Internet Things J. 1. http://dx.doi.org/10.1109/JIOT.2022.3151359.
Xu, H., Huang, W., Zhou, Y., Yang, D., Li, M., Han, Z., 2021a. Edge computing resource allocation for unmanned aerial vehicle assisted mobile network with blockchain applications. IEEE Trans. Wireless Commun. 20 (5), 3107–3121. http://dx.doi.org/10.1109/TWC.2020.3047496.
Xu, L.D., Lu, Y., Li, L., 2021b. Embedding blockchain technology into IoT for security: A survey. IEEE Internet Things J. 8 (13), 10452–10473. http://dx.doi.org/10.1109/JIOT.2021.3060508.
Yang, T., Cui, Z., Alshehri, A.H., Wang, M., Gao, K., Yu, K., 2022. Distributed maritime transport communication system with reliability and safety based on blockchain and edge computing. IEEE Trans. Intell. Transp. Syst. 1–11. http://dx.doi.org/10.1109/TITS.2022.3157858.
Yang, W., Guan, Z., Wu, L., Du, X., Guizani, M., 2021. Secure data access control with fair accountability in smart grid data sharing: An edge blockchain approach. IEEE Internet Things J. 8 (10), 8632–8643. http://dx.doi.org/10.1109/JIOT.2020.3047640.
Yang, R., Yu, F.R., Si, P., Yang, Z., Zhang, Y., 2019. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Commun. Surv. Tutor. 21 (2), 1508–1532. http://dx.doi.org/10.1109/COMST.2019.2894727.
Yi, S., Li, C., Li, Q., 2015. A survey of fog computing: concepts, applications and issues. In: Proceedings of the 2015 Workshop on Mobile Big Data. pp. 37–42.
Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Nguyen, T.H., Liu, F., Hewa, T., Liyanage, M., et al., 2020. 6G white paper: Research challenges for trust, security and privacy. http://dx.doi.org/10.48550/ARXIV.2004.11665, arXiv URL: https://arxiv.org/abs/2004.11665.
Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J., Yang, X., 2017. A survey on the edge computing for the internet of things. IEEE access 6, 6900–6919.
Yuan, L., He, Q., Chen, F., Zhang, J., Qi, L., Xu, X., Xiang, Y., Yang, Y., 2022. Csedge: Enabling collaborative edge storage for multi-access edge computing based on blockchain. IEEE Trans. Parallel Distrib. Syst. 33 (8), 1873–1887. http://dx.doi.org/10.1109/TPDS.2021.3131680.
Zhang, D., Yu, F.R., Yang, R., 2022. Blockchain-based multi-access edge computing for future vehicular networks: A deep compressed neural network approach. IEEE Trans. Intell. Transp. Syst. 23 (8), 12161–12175. http://dx.doi.org/10.1109/TITS.2021.3110591.
Zhang, L., Zou, Y., Wang, W., Jin, Z., Su, Y., Chen, H., 2021. Resource allocation and trust computing for blockchain-enabled edge computing system. Comput. Secur. 105, 102249. http://dx.doi.org/10.1016/j.cose.2021.102249, URL: https://www.sciencedirect.com/science/article/pii/S0167404821000730.
Zheng, Q., Li, Y., Chen, P., Dong, X., 2018. An innovative IPFS-based storage model for blockchain. In: 2018 IEEE/WIC/ACM International Conference on Web Intelligence. WI, pp. 704–708. http://dx.doi.org/10.1109/WI.2018.000-8.
Ziegler, V., Schneider, P., Viswanathan, H., Montag, M., Kanugovi, S., Rezaki, A., 2021. Security and trust in the 6G era. IEEE Access 9, 142314–142327. http://dx.doi.org/10.1109/ACCESS.2021.3120143.

Tri Nguyen was born in Ho Chi Minh, Vietnam, in 1993. He received the B.Sc. degree in computer science from the University of Information Technology - Vietnam National University, Vietnam in 2015, and the M.Sc. degree in computer science from the University of Pisa, Italy, in 2018. Since 2018, he has been a doctoral student in the Center for Ubiquitous Computing, University of Oulu. His research interests include distributed systems, blockchain technology, and information security.

Huong Nguyen was born in Ha Noi, Vietnam in 1995. Since August 2022, she has been a Ph.D. student at the Center of Ubiquitous Computing (UBICOMP) at the University of Oulu, Oulu, Finland. Before that, Huong completed her M.Sc. degree in Computer Science and Engineering at the University of Oulu in the same year and got a B.S in Computer Science at the Posts and Telecommunications Institute of Technology (PTIT), Ha Noi, Vietnam in 2018. Her main research interests are robot vision, intelligent transportation, Internet of Things, vulnerabilities in distributed systems, and edge computing.

Dr. Tuan Nguyen Gia received the Ph.D. degree in technology. He has published more than 60 international peer-reviewed articles. He is working on edge and fog computing, and edge-AI. His research interest is e-health, drones, autonomous and embedded systems, smart cities, and blockchain. He is also working on reconfigurable computing with FPGA and CGRA, energy efficiency of wearable devices and remote monitoring systems. He is also a Topic Editor of Vehicles, Future Internet and Sensors journals.