IoT with Blockchain: A New Infrastructure Proposal

Henry Hexmoor and Ebrahim Maghsoudlou
Department of Computer Science
Southern Illinois University, Carbondale, IL, USA
hexmoor@cs.siu.edu, ebrahim.maghsoudlou@siu.edu

Abstract

The convergence of the Internet of Things (IoT) and blockchain technology represents a pivotal evolution in the digital ecosystem, offering unprecedented opportunities to enhance security, transparency, and efficiency. This paper explores the synergistic potential between IoT and blockchain, aiming to shed light on their dynamic interplay and the prospects it holds for crafting a unified framework. By analyzing the inherent challenges and opportunities within IoT systems and the transformative capabilities of blockchain, we propose a conceptual architecture that could serve as a foundation for future research and development. Our exploration presents a visionary proposal, suggesting pathways for integrating these technologies to realize a robust, scalable, and secure infrastructure for the next generation of IoT applications. This work invites the academic and industrial communities to envision and contribute to the development of innovative solutions that leverage the strengths of both IoT and blockchain, paving the way for a more connected and secure digital future

1 Introduction

Internet of things (IoT) has gained popularity in our everyday lives. Tings include vehicles, appliances, electronic gadget, as well as online computational services and agents. In part, IoT things dwell in the cyberspace with limited computation and meager power resources. Therefore, things are often arranged to cooperate and pool their resources. Things are at the network edge. In order to coordinate and communicate, they must rely on nearby exchange sources such as roadside units for on road vehicles and local fog units as in the case of health care facilities.

Interaction rates among components of IoT are often at high volume and require rapid interaction among physical systems that exchange of information among IoT systems. Spatial and temporal information of a data exchange among IoT are location sensitive [1]. Given the availability, volatility, and speed of IoT information exchange, it is necessary to track relevance, validity, and freshness of data. Information must be verifiable, traceable, and immutable. Data validity and exchange must be time and place stamped [2, 3]. Blockchain offers transactions grouped into blocks with each block of data containing unique hash value for recording a historic timestamp assuring data traceability. Information flow in IoT must maintain integrity and trust. Security and privacy of transactions need to be preserved. Transactions need to be attributed to data generators and data consumers that are immutable [2, 4]. Blockchain utilizes encryption algorithms, hash functions, and digital signatures ensure quality and integrity of IoT data. The style of IoT interoperability is a salient feature of peer-topeer systems (P2P) [5]. Nodes of a blockchain form a distributed P2P network. A node that solves a problem is given the miner role with permission to append the validated block to the blockchain. The node broadcasts to the blockchain system and other nodes validating and updating the new results.

Finally, IoT information flow is often fully distributed and must possess an involuntary pattern free from central control that is the hallmark of autonomic processes found in biological systems. Blockchain smart contracts feature of blockchain systems accommodate autonomic information flow in IoT. Contract terms in smart contracts are executed automatically when a predetermined condition is satisfied. P2P spreads contracts in the network and the received contracts are saved in memory by the verification code and waits for the contract to be triggered by the process.

Meaningful functions are performed within the context of limited time intervals and bound to geospatial location as well as details of local events. Local entities form peer to peer networks and may operate over a local cloud. Operations that require detailed synthesis and computation will access distant resources over central clouds [6]. These criteria naturally fit a multistage blockchain. We endeavor to conceive of a framework for IoT that employs blockchain.

Section 2 will review blockchain and internet things. Section 3 offer our design ideas about combining IoT and blockchain. We offer some observations in the concluding section.

2 Background

The tapestry of modern technology includes prominent threads shaping the digital landscape and redefining the way we perceive and interact with the world. Those are the IoT and the Blockchain. The IoT envisions a world where every device, from the household refrigerator to the car, communicate in an interconnected network. The Blockchain promises a revolution in how we handle data ensuring transparency, security, and decentralization [3, 6]. This brief background section delves into these transformative technologies, offering an introduction to the IoT and the Blockchain. We will uncover the foundational elements of these technologies and explore their significance in our ever-evolving digital.

IoT, encompasses a system where everyday items can "message" each other through the internet. Imagine a world where the refrigerator tells you when you're out of milk, or your car requests the house to turn on the heating before you arrive. This is the world of IoT. IoT highlights the connection among everyday objects through the internet, making them smart and more pragmatic. Such connections yield benefits for how we live and work and their significance in today's digital world.

Looking back at its origins, the idea for objects communicating is not novel. The term "Internet of Things" was first coined in 1999 by Kevin Ashton. However, before that, in the 1980s and 1990s, we already had simple systems that hinted this idea. An example from the 1990s is the Coke machine connected to the internet at a university. It was one of nascent IoT. As more people started using the internet in the 2000s, more devices were interconnected with extensions that has made IoT a major part of our lives today affecting many areas like homes, healthcare, transport, and farming [7].

Consider sensors and actuators. Sensors gather information from the world, like temperature or light., On the other hand, actuators perform actions based on collected information. For example, if a sensor detects that it is too hot, an actuator might turn on a fan. Another important piece in this IoT puzzle is known as the edge devices. These are special because they process information in the field, instead of sending data far away to computer. This makes things faster and saves energy. Imagine a camera that can detect someone at the door and then quickly send a picture. This camera is acting like an edge device because it processes the image in the field and then shares it with you. All these devices work together, making the IoT world function smoothly and helping us in many ways in our daily lives.

Efficient and effective communication among IoT devices is paramount. This communication hinges on specific standardized rules or protocols, ensuring that the exchange of information is consistent and reliable. Among the myriad of protocols available, two particularly stand out for their relevance and utility in IoT applications: MQTT and CoAP [2].

MQTT (Message Queuing Telemetry Transport) originated as a lightweight messaging protocol optimized for conditions where network bandwidth is at a premium. Characterized by its publish/subscribe communication model, MQTT is designed for asynchronous communication between devices, making it exceptionally suitable for environments where a consistent network connection is not guaranteed. Its lightweight header and quality of service levels make it adaptable, ensuring message delivery even in unstable conditions.

On the other hand, CoAP (Constrained Application Protocol) is a web transfer protocol, designed explicitly for use with constrained nodes and constrained networks in the IoT. It operates over User Datagram Protocol (UDP) and employs a request/response communication model. CoAP's primary strength lies in its lightweight nature, allowing it to function effectively on devices with limited processing capabilities and power availability. Its built-in discovery mechanism and interoperability with HTTP also make it a versatile choice for various IoT scenarios.

Comparatively, the choice between MQTT and CoAP hinges on the specific requirements of the IoT application in question. For scenarios necessitating consistent message delivery in less stable networks, MQTT's robustness proves advantageous. Conversely, CoAP, with its low overhead and adaptability, shines in environments where device resources are limited, and energy efficiency is a priority.

Understanding the nuances of these protocols is essential for optimizing IoT network performance, as each brings its unique strengths to cater to the diverse challenges presented by different IoT environments [8].

The ascent of the Internet of Things (IoT) has unlocked numerous potentials, shaping diverse industries from healthcare to urban planning. Yet, this meteoric rise isn't without its set of obstacles. Central among these are the challenges and security concerns that threaten to hamper the growth and trust in IoT systems.

Traditional IoT Networks have inherent challenges, including the following [2]:

- **Heterogeneity:** The diverse range of devices, each with varying software and firmware, makes consistent security implementations tough.
- **Resource Constraints:** Many IoT devices, designed for minimal power usage and computational activities, often lack robust security features.
- **Lack of Standards:** The IoT ecosystem, being relatively nascent, lacks universal standards, leading to inconsistent security practices.
- **Continuous Operation:** Devices that operate incessantly without human interaction make anomaly detection difficult.

These technical challenges have real-world ramifications, most notably when we consider the consequences of security breaches summarized herein [5, 9]:

- **Physical Harm:** Unlike traditional cyber-infrastructures, compromised IoT systems can lead to physical damages. Examples include smart home devices causing unintended accidents or hacked healthcare gadgets endangering lives.
- **Data Privacy:** Personal data harvested from IoT devices can be exploited if they are not properly protected.

- **Infrastructure Disruption:** Breaches in the smart grid systems or urban infrastructures can cause broad societal disturbances.
- **Economic Costs:** firms can encounter financial losses from product recalls or lawsuits due to compromised IoT devices.

The implications extend beyond digital realms. For instance, a security loophole in a smart thermostat might result in unsafe home temperatures, while compromised medical devices can pose life-threatening risks. These scenarios emphasize that in the realm of IoT, the boundary between digital vulnerabilities and real-world consequences is often blurred.

The promise of IoT is immense, but the road ahead demands vigilant attention to its challenges and security pitfalls. As the IoT paradigm continues to evolve, ensuring its resilience and safety becomes paramount, not just for digital sanctity but also for real-world well-being.

Blockchain is like a digital ledger or a logbook. Imagine a book that records every transaction or every event. Once recorded, it becomes very difficult to alter. Many copies are maintained by distinct individuals. Asynchronously and independently, many individuals may verify veracity of recorded content.

The salient features of blockchain are the following[10]:

- **Blocks and Chains:** Blockchain consists of many "blocks". Each block stores information. These blocks are linked or "chained" together in sequential order. Any change in a block affect all the blocks after it. This continuity is part of its security [11].
- **Public Ledger:** Blockchain is like a public logbook. Many people may examine the contents. This means that any attempt at alteration is witnessed by others. This creates attack deterrence [12].
- **Decentralization:** Instead of a central authority, blockchain is distributed over a network of peers. Multiple blockchain copies exist. Many nodes must concur for any change to take place. This creates attack resistance [13].
- **Proof of Work:** In a public blockchain, a new block is added strictly when a kind of a difficult puzzle is solved that is known as the proof of work. This creates a deliberateness in new information augmentation.

There are several different kinds of blockchains outlined:

- **Public Blockchains:** These are open to public participation. Bitcoin is the most widely known example.
- **Private Blockchains:** Participation is limited to credentialed private individuals of a group such as organizations that require privileged control.
- **Consortium Blockchains:** This is suitable for several organizations with a shared interest or shared resources.

For the IoT, blockchain provides very useful features outlined herein:

- **Decentralization:** The command and control is not centralized. This ameliorates against attacks.
- **Transparency**: Most blockchains let everyone see the information. This means if something wrong happens, it can be spotted quickly.

- **Immutability:** Once something is added to the blockchain, it's very hard to change. This keeps the information safe and true.
- **Consensus Mechanisms**: This is a way for everyone to agree on what's true. There are rules about how information is added. Everyone must agree based on these rules.

We will argue that blockchain features will provide security for the IoT.

3 Proposed IoT-BC Architecture

In an era marked by rapid technological progression, the fusion of IoT with Blockchain presents a promising trajectory for the digital demand. This convergence addresses the escalating growth of IoT devices, requiring enhanced security and efficient data management. By intertwining these technologies, our proposed framework heralds a comprehensive blueprint design that amalgamates various IoT applications from smart homes to the industrial grids, within a homogenous infrastructure [7, 14]. Central to this design is the IoT-BC Gateway, serving as a pivotal node in managing diverse communication aspects, and the overarching IoT-BC Cloud, which shoulders extensive network responsibilities from data analytics to potential cryptocurrency initiatives. This introduction delves into the intricate facets and profound potential of our novel sketch [15].

As the interplay between the IoT and blockchain continues to garner attention in the academic and industrial worlds, our proposed framework seeks to bridge the existing gaps and present an integrated solution [16]. By harnessing the unique attributes of both technologies, the architecture sets a precedent for creating a resilient and scalable IoT-blockchain ecosystem. Herein, we elucidate the core tenets of this innovative delineation [17, 18]:

- **Unified Approach:** Our conception harmoniously combines the myriad functionalities of IoT — from household applications in smart homes to expansive realms like smart cities and industries. This synthesis constitutes the foundational aspect of our topological framework.

- **Significance of IoT-BC Gateways:** Central to the architecture are the IoT-BC Gateways. Renowned for their versatile processing capacity, they adeptly manage data influx from assorted IoT devices. Leveraging blockchain's inherent algorithms, these gateways play pivotal roles in block formation and the all-important consensus mechanism.

- **Modular Zonal Structure:** The design introduces a zonal modular system. Each IoT-BC Gateway delineates a distinct "zone" fostering efficient communication amongst devices within its domain. However, the zenith of this architecture is realized in the seamless connectivity between these zones culminating in an seamless network fabric.

- **Oversight through IoT-BC Cloud:** Beyond the zonal configurations stands the superior IoT-BC Cloud. Serving as the nucleus of the entire framework, this entity undertakes a multitude of tasks—ranging from data analytics and user management to cryptocurrency interfaces—underscoring its pivotal role in the ecosystem.

- **Security Paradigm:** The proposed topology remains uncompromising on security. Each gateway operates within a fortified encrypted enclave, with inter-gateway communications undergoing meticulous vetting by the IoT-BC Cloud, ensuring a fortified environment that is impervious to external threats[19].

Figure 1 is an illustrative block diagram depiction capturing high level symbiotic relationships and interactions.

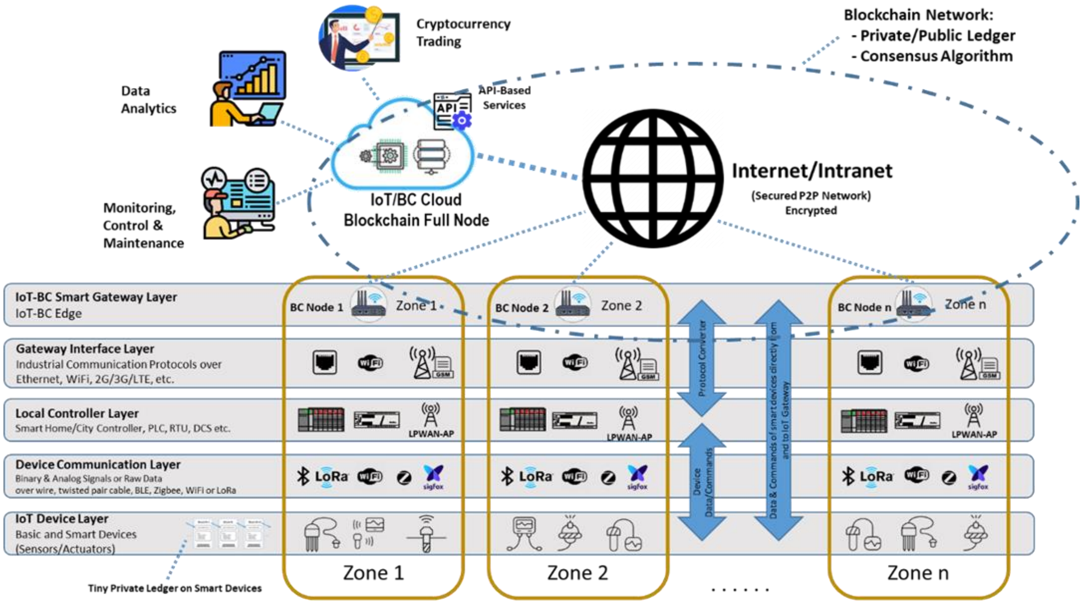
Cryptocurrency Trading
Blockchain Network:
- Private/Public Ledger
- Consensus Algorithm
Data Analytics
API-Based Services
API
Internet/Intranet
(Secured P2P Network) Encrypted
Monitoring, Control & Maintenance
IoT/BC Cloud Blockchain Full Node
IoT-BC Smart Gateway Layer
IoT-BC Edge
BC Node 1
Zone 1
BC Node 2
Zone 2
BC Node n
Zone n
Gateway Interface Layer
Industrial Communication Protocols over Ethernet, WiFi, 2G/3G/LTE, etc.
GSM
Local Controller Layer
Smart Home/City Controller, PLC, RTU, DCS etc.
LPWAN-AP
Device Communication Layer
Binary & Analog Signals or Raw Data over wire, twisted pair cable, BLE, Zigbee, WiFi or LoRa
LoRa
sigfox
IoT Device Layer
Basic and Smart Devices (Sensors/Actuators)
Protocol Converter
Device Data/Commands
Data & Commands of smart devices directly from and to IoT Gateway
Tiny Private Ledger on Smart Devices
Zone 1
Zone 2
Zone n
. . . . . .

Figure 1 - Proposed IoT-BC Architecture

The diversity and multitude of IoT devices present a compelling exploration. By classifying these devices, we can understand their distinct functionalities and roles within the wider IoT ecosystem, thereby facilitating more effective integration into our scaffolding. This section delves into the nuanced categorizations of IoT devices, highlighting their intrinsic and extrinsic characteristics [20].

- **Basic Devices:** At one end of the spectrum, we have elementary devices, often termed as 'basic'. These gadgets, such as domestic thermostats or rudimentary sump pumps, are constrained in their hardware capabilities. Typically, they execute singular tasks, producing simple binary or analog signals. Given their intrinsic limitations, these devices usually necessitate external controllers for operational efficacy.
- **Smart Devices:** Ascending the complexity ladder, we encounter the 'smart' devices. Infused with moderate computational prowess and embedded electronic systems, these devices distinguish themselves with enhanced functionality. Characterized by storage capacities in the realm of tens of megabytes and equipped with 8-bit or 32-bit microcontrollers, they exhibit greater adaptability. Their processing units, although not high-end, range from modest 10 KHz frequencies to sub-1GHz levels. Notably, these devices, being recent additions to the IoT fold, are capable of handling elementary blockchain-related tasks. Their ability to implement lightweight cryptographic techniques

is particularly salient. Some of the commonly adopted lightweight hashing and encryption algorithms for such embedded devices include PHOTON, SPONGNET, PRESENT, SIMON, SPECK etc [20, 21].

A noteworthy aspect of these smart devices is their capability to instantiate private ledgers. Essentially, these small-scale private ledgers function as diminutive databases, archiving a historical trail of data generated by the device. These smart devices are adept at transmitting their most recent data blocks to IoT-BC gateways directly. The employment of communication interfaces like LTE, 5G [22], LPWAN, WiFi, Zigbee, and BLE, in conjunction with communication protocols such as MQTT and COAP, make this feasible [23, 24]. Additionally, light-weight encryption protocols fortify the data transmission, ensuring its integrity and security. For a visual representation detailing the architecture of the private ledger generated by IoT smart devices, readers are directed to Figure 2.

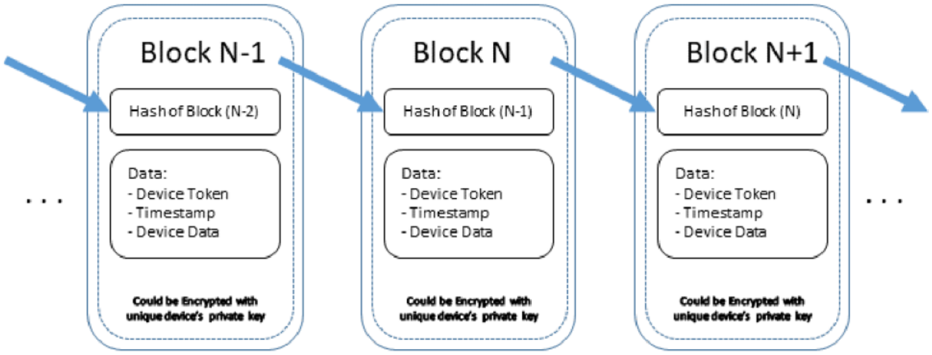

Figure 2 - Private Tiny Ledger for each Smart Device

In the constantly evolving landscape of the IoT and blockchain integration, the prominence of specialized gateways becomes increasingly vital. These gateways, referred to herein as IoT-BC Smart Gateways, serve as pivotal points of connection, data aggregation, and processing between the diverse realms of IoT networks and the immutable nature of blockchain technology. This section elucidates the multifaceted role of these Smart Gateways within our proposed topology.

1. **Comprehensive Connectivity:** Central to the efficacy of IoT-BC Smart Gateways is their ability to facilitate seamless integration. They support an expansive array of both wired and wireless communication interfaces prevalent in modern Industrial and IoT-focused networks. Whether it's through conventional telecommunication mediums like Ethernet, WiFi, and LTE or through low-power, wide-area network (LPWAN) technologies like LoRa and Zigbee, these gateways ensure uninterrupted data exchange.

2. **Protocol Versatility:** Beyond mere connectivity, IoT-BC Smart Gateways are equipped to comprehend and communicate using a diverse set of industry-standard protocols. This includes but is not limited to protocols like DNP3, IEC 60850, MQTT, and COAP. Whether interacting with a Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), or Smart Grid, the gateway's proficiency in these protocols enables fluid data interchange.

3. **Blockchain Edge Processing:** One of the salient features of the IoT-BC Smart Gateways is their capability to function as Blockchain Edge Devices. By gathering comprehensive data from various IoT sources, these gateways can construct blocks, manage consensus algorithms, and address other pertinent blockchain-related tasks. Each gateway, in essence, delineates a distinct zone within the network, allowing intra-zone nodes to interact seamlessly.
4. **Secure Data Transmission:** With data being the lifeblood of both IoT and BC, ensuring its security during transmission is paramount. IoT-BC Smart Gateways, in their strategic position between the IoT and BC realms, ensure this data is transmitted over secure lines, be it within the vast expanses of the internet or the more controlled environment of intranets.
5. **Centralized IoT-BC Interface:** The proposed topology places the IoT-BC Smart Gateways as a vital bridge between localized data collection points and the overarching IoT-BC Cloud, which acts as the full node in the network. This central interface not only aggregates data but also offers avenues for data analytics, operational monitoring, and user management, among other services.

IoT-BC Smart Gateways, as conceptualized in our proposed topology, are not mere data conduits. They are intelligent, versatile, and secure devices equipped to handle the complexities and nuances of integrating vast IoT networks with the stringent requirements of blockchain technology. Their role, as illustrated in Figure-3, is pivotal to the success and efficiency of the integrated IoT-BC network model.

The synthesis of IoT and blockchain technologies requires a strategic fusion of the dynamic capabilities of IoT with the security and trustworthiness intrinsic to blockchain. Our proposed structure seeks to leverage the strengths of both domains, culminating in a system that stands apart from traditional models. Below, we enumerate the multifaceted advantages that are a result of our innovative IoT-BC network topology design.

1. **Enhanced Security:** Our topology, bolstered by the blockchain foundation, ensures that every transaction remains immutable, thus safeguarding data integrity and curtailing risks associated with data tampering. Furthermore, the dedicated communication lines that connect IoT devices, smart gateways, and the IoT-BC Cloud are encrypted, offering superior data privacy and a robust defense against potential cyber threats.
2. **Universal Compatibility:** Designed with an agnostic stance to the wide array of existing communication protocols, our topology guarantees an unproblematic integration with both current and future IoT systems. Moreover, the architecture's inherent flexibility allows for easy addition or modification, making it a resilient solution even in the face of rapid technological advancements in the IoT domain.
3. **Scalability and Flexibility:** The modular essence of our topology permits efficient scalability, capable of accommodating an ever-growing number of IoT devices without necessitating substantial changes. Additionally, the strategy of demarcating specific zones, overseen by IoT-BC Gateways, ensures localized scalability, thereby streamlining the management of heavily populated IoT networks.
4. **Resource Efficiency:** By allocating the majority of blockchain-related computational tasks to the gateway level, the topology effectively diverts demanding operations away from the resource-constrained IoT devices. This ensures their optimal performance. Furthermore, the capability of smart IoT devices to maintain private ledgers facilitates localized data storage, thus reducing the demand for incessant communication with the main blockchain.

5. **Mobility and Continuity:** Our topology is adept at providing seamless transition of mobile IoT devices between different operational zones. This ensures that data transmission and processing remain uninterrupted, even as devices transition from the influence of one IoTBC Gateway to another.
6. **Comprehensive Centralized Services:** The centralized nature of the IoT-BC Cloud offers a unified platform for data access across the entire network, making tasks such as monitoring, analytics, and control more streamlined. The inclusion of cryptocurrency trading services within the topology presents innovative opportunities for monetizing IoT operations, thus heralding new business avenues.

The topology we propose is a conceptual sketch that is n adaptable and efficient model poised to usher in the IoT and blockchain amalgamation. The advantages we've elucidated underscore the topology's potential in reshaping contemporary paradigms and setting new benchmarks in IoT-BC synergy.

4 Conclusions

In this paper, we have explored the promising synergy between the Internet of Things (IoT) and blockchain technology, highlighting how their integration can address critical challenges and unlock new potentials in secure, decentralized systems. By proposing a novel architecture, IoT-BC, we aim not only to enhance the security and efficiency of IoT networks but also to provide a scalable, interoperable framework that supports the diverse requirements of IoT applications. This exploratory work lays the groundwork for a new paradigm in IoT infrastructure, emphasizing the importance of blockchain in achieving a robust, transparent, and efficient ecosystem. Our proposal serves as a foundational reference for future research, development, and implementation of IoT-blockchain systems, paving the way for innovative solutions that leverage the strengths of both technologies to meet the evolving demands of the digital world.

5 References

[1] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT," in *2018 ieee international conference on pervasive computing and communications workshops (percom workshops)*, 2018: IEEE, pp. 197-202.

[2] C. Sobin, "A survey on architecture, protocols and challenges in IoT," *Wireless Personal Communications,* vol. 112, no. 3, pp. 1383-1429, 2020.

[3] B. Alamri, K. Crowley, and I. Richardson, "Blockchain-based identity management systems in health IoT: A systematic review," *IEEE Access,* vol. 10, pp. 59612-59629, 2022.

[4] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications,* vol. 28, no. 1, pp. 296-312, 2023.

[5] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, and H. Arshad, "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers & Security,* vol. 112, p. 102494, 2022.

[6] M. A. I. Mozumder, M. M. Sheeraz, A. Athar, S. Aich, and H.-C. Kim, "Overview: Technology roadmap of the future trend of metaverse based on IoT, blockchain, AI technique, and medical domain metaverse activity," in *2022 24th International Conference on Advanced Communication Technology (ICACT)*, 2022: IEEE, pp. 256-261.

[7] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Computing Surveys (CSUR),* vol. 53, no. 1, pp. 1-32, 2020.

[8] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future generation computer systems,* vol. 88, pp. 173-190, 2018.

[9] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks,* vol. 4, no. 3, pp. 149-160, 2018.

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

[11] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Transactions on Services Computing,* vol. 15, no. 4, pp. 2490-2510, 2020.

[12] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, 2016, vol. 310, no. 4: Chicago, IL, pp. 1-4.

[13] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications,* vol. 10, pp. 983-994, 2017.

[14] F. Viel, L. Augusto Silva, V. R. Q. Leithardt, J. F. De Paz Santana, R. Celeste Ghizoni Teive, and C. Albenes Zeferino, "An Efficient Interface for the Integration of IoT Devices with Smart Grids," *Sensors,* vol. 20, no. 10, p. 2849, 2020.

[15] L. Da Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," *IEEE Internet of Things Journal,* vol. 8, no. 13, pp. 10452-10473, 2021.

[16] L. Yang, W. Zou, J. Wang, and Z. Tang, "EdgeShare: A blockchain-based edge data-sharing framework for Industrial Internet of Things," *Neurocomputing,* vol. 485, pp. 219-232, 2022.

[17] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, 2017: IEEE, pp. 618-623.

[18] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of IoT using blockchain technology," *IEEE Internet of Things Journal,* vol. 8, no. 2, pp. 881-888, 2020.

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

[20] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," *IEEE Access,* vol. 9, pp. 28177-28193, 2021.

[21] M. E.-H. M. C. A. F. A. Serhrouchni, "Analysis of Cryptographic Algorithms on IoT Hardware platforms," presented at the 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, France, 2018.

[22] M. Saedi, A. Moore, and P. Perry, "Synthetic Generation of Realistic Signal Strength Data to Enable 5G Rogue Base Station Investigation in Vehicular Platooning," *Applied Sciences,* vol. 12, no. 24, p. 12516, 2022.

[23] L. Tightiz and H. Yang, "A comprehensive review on IoT protocols' features in smart grid communication," *Energies,* vol. 13, no. 11, p. 2762, 2020.

[24] A. Souri, A. Hussien, M. Hoseyninezhad, and M. Norouzi, "A systematic review of IoT communication strategies for an efficient smart environment," *Transactions on Emerging Telecommunications Technologies,* vol. 33, no. 3, p. e3736, 2022.