A Blockchain Application Prototype for the Internet of Things

Mansour Mededjel, Ghalem Belalem, Fatima Zohra Nesrine Benadda, and Samah Kadakelloucha

Original scientific article

***Abstract*—The emergence of the Internet of things (IoT), associated with the explosion in the number of connected objects, and the growth in user needs, makes the Internet network very complex. IoT objects are diverse and heterogeneous, which requires establishing interoperability and efficient identity management on the one hand. On the other hand, centralized architectures such as cloud-based ones can have overhead and high latency, with a potential risk of failure. Facing these challenges, Blockchain technology, with its decentralized architecture based on a distributed peer-to-peer network, offers a new infrastructure that allows IoT objects to interact reliably and securely. In this paper, a new approach is proposed with a three-layer architecture: layer of sensing and collection of data made up of the IoT network, layer of processing and saving of data exchanges at the Blockchain level, and access and visualization layer via a web interface. The prototype implemented in this study allows all transactions (data exchanges) generated by IoT devices to be recorded and stored on a dedicated Blockchain, assuring the security of IoT objects' communications. This prototype also enables access to and visualization of all data and information, thus enhancing the IoT network's transparency.**

***Index terms*—Internet of things, Blockchain, Decentralization, Publish/Subscribe model, Transparency, Security.**

I. Introduction

The exponential growth in the number of connected objects has revealed new insights into the impact of the Internet of Things (IoT) technology in several areas. Smart cities, machine-to-machine (M2M) systems, connected vehicles, and wireless sensor networks (WSNs) are just a few of the topics covered. Today, the development and integration of numerous technologies and concepts enable IoT to create a new technological dimension by removing the borders between the real and the virtual worlds. Cloud computing, Big Data, and Blockchain are among the key technologies related to the IoT.

Despite their obvious benefits, most IoT applications face many challenges in the real world due to their centralized architecture and the huge number of devices. One example is data and communication security issues. In the centralized approach, all devices are connected and authenticated through a server, leading to a single point of failure. Therefore, moving from a centralized to a decentralized approach can help overcome many issues and challenges discussed later in this paper (see Section III.C). In this situation, Blockchain as a disruptive technology can be a crucial enabler for solving many IoT-related issues.

In this regard, this paper discusses a Blockchain-IoT integration approach aiming to solve some issues and challenges that face an IoT system, namely data security and integrity, transparency, and the identity of connected objects. A three-layer architecture is proposed in this approach: the Blockchain, the IoT network, and the web interface that allows users to interact with the two previous layers. MQTT (Message Queuing Telemetry Transport), a lightweight publish/subscribe messaging protocol, is used for communicating the IoT-generated data to the Blockchain. The contribution of this study is the use of the full Blockchain nodes as MQTT brokers in the communication process between IoT devices and the Blockchain. On the one hand, this permits overcoming the resource constraint of IoT devices in processing and storing the acquired data while ensuring their security and integrity, on the other hand.

The rest of this paper is organized as follows. Section II reviews and compares some related work in this area. Sections III and IV describe the IoT and Blockchain technologies. Section V discusses the current convergence between the two technologies, their implications, and related challenges and solutions. Section VI and VII present the proposed architecture with a prototype implementation of Blockchain for an IoT network. Finally, Section VIII concludes this work.

II. Related Work

Most of the related works on Blockchain-IoT integration can be classified according to their purpose, including architecture, smart contracts, consensus algorithms, and security.

Reyna et al. [39] provided a comprehensive overview of the connection between Blockchain and IoT, as well as an analysis of the major issues that both technologies must overcome to function together. They also evaluated the feasibility of using Blockchain nodes on IoT devices and identified key areas where Blockchain could impact IoT development.

Lo et al. [25] conducted a systematic literature review to analyze how Blockchain has been applied to IoT to address the challenges of centralized key management, lack of standards, the integrity of things' states, limited thing computation

Manuscript received December 1, 2021; revised February 12, 2022. Date of publication April 8, 2022. Date of current version April 8, 2022. The associate editor prof. Claudia Canali has been coordinating the review of this manuscript and approved it for publication.

M. Mededjel, F. Z. N. Benadda and S. Kadakelloucha are with the Department of Mathematics and Computer Science, Faculty of Science and Technology, University of Ain Temouchent Belhadj Bouchaib, Algeria.

G. Belalem is with the Department of Computer Science, Faculty of Exact and Applied Sciences, University Oran1 Ahmed Ben Bella, Oran, Algeria (e-mails: mansour.mededjel@univ-temouchent.edu.dz, {nesrinebenadda0, crowiliza, ghalem1dz}@gmail.com).

Digital Object Identifier (DOI): 10.24138/jcomss-2021-0129

capability, and interoperability between things. The authors identified that performance and scalability are the main problems while integrating Blockchain with IoT platforms due to the high volume of data collected by IoT things. Besides, the authors provided their insights on improving the existing solutions, research methodology, and factors to consider when integrating Blockchain with IoT.

Atlam et al. [4] discussed the integration of Blockchain and IoT, highlighting benefits such as decentralization, resiliency, and security, as well as challenges such as scalability and storage concerns.

Miraz [30] proposed the concept of Blockchain of Things (BCoT) by discussing the feasibility and limitations of combining Blockchain with IoT technology. Authors consider that IoT and Blockchain technologies have distributed and autonomous properties, which reveal the great potential to work together, acting as complements. They also presented a detailed literature survey covering a wide range of projects and research on the integration concept of these two technologies.

Pavithran et al. [34] conducted a literature review and analysis on Blockchain technology applications in IoT while recommending a framework for this applications environment. After identifying and explaining the key components and challenges to consider, the authors evaluated the generic Blockchain framework for applications in IoT by simulating two Blockchain implementations. They concluded that device-to-device architecture performs better than gateway-based implementations.

Ferdous et al. [14] described in their study an evaluation framework for selecting the suitable Blockchain platform for IoT applications.

Dedeoglu et al. [12] studied the primary benefits and design challenges of Blockchain technology for IoT applications. The authors provided some use case examples with a detailed description of the different types, architectures, and consensus mechanisms used in Blockchain to solve IoT issues.

Tseng et al. [47] proposed an architecture that implements Blockchain in managing heterogeneous IoT systems, along they discussed challenges in integration and development.

Xiong et al. [49] suggested a general paradigm for the architecture design of Blockchain-enabled IoT systems, in which transaction data among IoT devices may be stored and managed using Blockchain technology. The authors discussed data management patterns, prospective application scenarios, and potential obstacles to the proposed Blockchain-enabled IoT system architecture. As a case study, they analyzed a learning-assisted resource allocation method for data transmission, with numerical results to show that the proposed scheme outperforms baseline schemes.

Saxena al. [41] presented a comprehensive survey on the integration trends of Blockchain technology with IoT and the insights of this new paradigm. In particular, they focused on how Blockchain technology can be utilized to solve the most relevant IoT security issues and highlighted the main benefits and risks of integrating Blockchain and IoT. The authors suggested that Blockchain technology is an ideal and most suitable candidate for empowering IoT and realizing a safe, convenient, supervisable, and transparent system that paves the way for new emerging business models. They also highlighted the most relevant Blockchain-based IoT applications and outlined some future research directions.

Table I compares our proposal to the above-reviewed papers within the scope of BC-IoT integration.

III. Internet of Things (IoT)

IoT is a network of multiple devices that communicate with one another without the need for direct human intervention. It facilitates the quick transfer of data in an efficient way. The IoT consists of devices that communicate to other devices, things, machines, or infrastructures. Things are physical or virtual objects capable of being integrated into the communication network [38].

A. The IoT Components

An IoT system typically consists of the following four components:

- Connected devices: These devices have detection, actuation, and data processing capabilities. They consist of one or more built-in sensors, and they have the potential to collect large volumes of data of different types like temperature, humidity, and position.
- Communication network: IoT uses standard protocols and wireless networking solutions. The most prominent wireless families of technologies, as illustrated in Table II, are LPWAN (Low Power Wide Area Networks), cellular networks (3G,4G, 5G), IEEE 802.15.4 Protocols or LR WPAN (Low-Rate Wireless Personal Area Networks) such as Zigbee, Bluetooth/BLE, and Wifi (Wifi halow, wifi6, ...) [5][9]. IoT networks have different connectivity requirements, so there is no one-size-fits-all solution. However, energy performance is crucial. The choice of such a network must generally consider the limits of objects' battery life, communication distance, and cost of service to allow more objects' connection.
- Data: These are of great value in IoT systems. They can be primary elements collected from objects or the result of an analysis process. Data should be stored in the device's local memory (if it has one). However, IoT devices have mainly low memory and low processing ability. Therefore, the cloud takes the authority to store this data in such a case [7].
- Applications: They are an abstraction of the IoT system that allows visualization of processed data and offers various services to users.

B. The IoT Architecture

The elementary architecture of an IoT system consists of three layers: the perception, network, and application layers [27][42].

- The perception or the physical layer: is essentially composed of a set of sensors and actuators. This layer is responsible for detecting physical parameters and identifying other surrounding objects.

TABLE I
COMPARISON OF RELATED WORKS

Paper	Scope and contribution type	Topic and research issues	Architecture type	Consensus algorithm	Security mechanism	Case study, application scenario
Reyna et al. [39]	A comprehensive overview of the possibility and issues of connecting Blockchain and IoT	- Challenges of integrating IoT and Blockchain and possible topologies for that integration - Blockchain potential benefits for the IoT - Blockchain-IoT applications and platforms	--	--	--	--
Lo et al. [25]	A systematic literature review analyzing the proposed solutions and methodologies used to integrate Blockchain with IoT	- Existing IoT issues and Blockchain-based solutions covering both data management and things management - Common design defects in the integration of Blockchain and IoT that are related mainly to performance and scalability	--	--	--	--
Atlam et al. [4]	An overview of integrating Blockchain with IoT system	- The benefits resulting from the integration process and the implementation challenges encountered	--	--	--	--
Miraz [30]	An analysis of the concept of Blockchain of Things (BCoT)	- IoT and Blockchain fundamentals - BCoT security	--	--	--	--
Pavithran et al. [34]	A literature review analysis on Blockchain technology in IoT	- Key components to consider and integration requirements for Blockchain and IoT - Evaluation of the generic Blockchain framework for applications in IoT	IoT-device-only and Gateway-based architecture	--	Elliptic curve and SHA-256	Simulation of a generic network with Cooja using IPv6 over 6LoWPAN for the communication process.
Ferdous et al. [14]	An evaluation framework for selecting the suitable Blockchain solution for IoT applications	- IoT applications' functional, security, and privacy requirements - Existing Blockchain platforms' intrinsic features - Evaluation framework based on a combination of IoT requirements and properties of Blockchain platforms	--	--	--	Four IoT application areas, namely healthcare, supply chain, smart city, and smart home have been explored.
Dedeoglu et al. [12]	A detailed description of various challenges, types of Blockchain, and architectures according to access, control, consensus mechanisms, and network structures	- Key benefits and design challenges of Blockchain technology for IoT - Applications areas and open issues for future research directions	--	--	--	Some potential use cases for Blockchain in IoT are discussed, such as smart cities, supply chains, sharing economy services, and insurance and liability services.
Tseng et al. [47]	Proposal of a perspective architecture that seamlessly integrates IoT and Blockchain to support and manage a large-scale heterogeneous IoT system	Key unsolved challenges concerning: - the management of heterogeneous IoT systems, and - the difficulty of integrating Blockchain and IoT	Seven-layer IoT reference model	PoS and PBFT protocols	--	--
Xiong et al. [49]	Proposal and analysis of a Blockchain-based data management system for IoT	- Data management patterns - Integration approaches - Application scenarios and potential challenges of Blockchain in IoT systems	A conceptual and general architecture framework combining Blockchain and IoT	--	--	A case study of a Blockchain-enabled IoT system under constrained resources with a learning-assisted data transmission scheme.
Saxena al. [41]	A comprehensive survey of the security enhancements made in IoT systems using Blockchain and the challenges that arise during integration	- Major security requirements and challenges in IoT - The motivation behind integrating Blockchain technology and IoT - Future research directions for open IoT security problems	--	--	--	Various Blockchain-based IoT applications are explored, including smart home, supply chain management, business models, security for smart cities, VANETs, and healthcare.
Our proposal	A proposal of a Blockchain-IoT integration prototype to overcome IoT devices' resource constraints regarding data processing and storage while ensuring security and integrity within the IoT network	Major issues and challenges faced by IoT systems, such as: - Data and communication security within IoT network - Resource limits - Data management - Identification of connected objects	Three-part architectural model	PBFT	RSA and SHA-256	Use case scenario based on a generic IoT network composed of mobile devices.

TABLE II
IoT WIRELESS TECHNOLOGIES COMPARISON [3][5][9][18][28][43]

		Data rate	Power consumption	Range	Cost
RFID		< 10 Mbps	low	10 cm - 100 m	low
Wi-Fi		1 Mbps – 6 Gbps	high	100 m	medium
NFC		424 Kbps	very low	< 10cm	low
Bluetooth		1 Mbps	low	< 10 m	low
BLE		1 Mbps	very low	10 m	medium
Zigbee		250 kbps	very low	100 m	low
Z-Wave		100 Kbps	very low	30 m	low
Wi-Fi HaLow		150 Kbps - 80 Mbps	medium	1 km	medium
LPWAN	LTE-M	1Mbps	medium	5 Km	high
	NB-IoT	250 kbps	very low	15 Km	low
	LoRa	50 kbps	low	20 Km	low
	Sigfox	100 bps, 600 bps	very low	40 Km	low
3G, 4G, 5G		2Mbps – 10 Gbps	high	>30km	high

- The network layer: provides connectivity between objects and devices in the system. This layer is also responsible for the transmission and processing of data generated from various devices.
- The application layer: provides user-specific services for the deployment of IoT applications, such as smart homes and smart cities, smart health, and intelligent transport. XMPP, DDS, AMQP, and REST are some of the protocols applied at this layer [1][17]. The two most used standard protocols are COAP (Constrained Application Protocol) and MQTT [46].

COAP is a client/server protocol like HTTP but mainly works over UDP, with reduced costs and a limited data block of 1024 bytes. To guarantee the delivery of packets over the network without using TCP, CoAP uses DTLS (Datagram Transport Layer Security). The latter is the building block of secure CoAP with which it can easily transport messages over lossy UDP connections and can still guarantee packets. CoAP, a secure resource-saving protocol, could be a good fit for IoT applications where mobile devices mostly use UDP to connect to the internet. MQTT is a Publish/Subscribe protocol in which the data sent by the objects (Publishers) are transferred to the MQTT server (Broker) that processes, stores, and publishes them to interested clients (Subscribers). Messages should be accessible for many device types by including, in their frame data, a message header type that is available for many devices. This broadcasting method is critical for IoT devices as they are small and battery-powered in most cases. MQTT thus serves a purpose in the field of IoT [17].

Both MQTT and CoAP are open standards, better suited to constrained environments than HTTP, provide mechanisms for asynchronous communication, run on IP, and have a range of implementations. Figure 1 presents the three-layer IoT architecture.

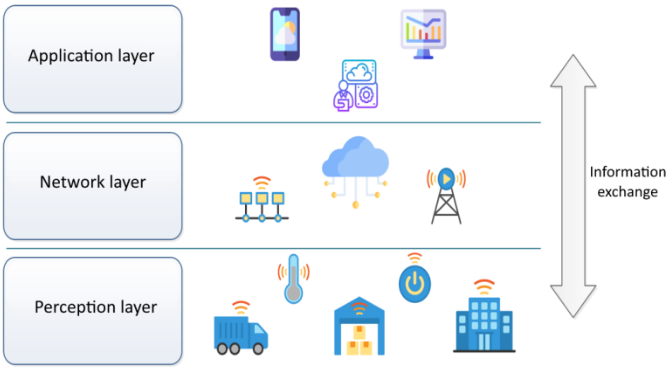


Fig. 1. The three-layer IoT architecture

C. IoT Issues and Challenges

Even though the benefits and solutions provided by IoT in different sectors are many, still challenges persist. Most of these challenges are related to the heterogeneity of IoT devices, communication protocols, and data. This section summarizes the main issues and challenges the IoT faces.

C.1 Security and Privacy

IoT paradigm encompasses today a wide range of devices with weak built-in security mechanisms. As a result, these devices are increasingly becoming an ideal target for cyber-attacks, which puts the issue of data security and privacy at the top of the challenges facing the IoT today. Regarding the architecture described above, some issues include jamming attack and Sybil attack at the physical level; replay or duplication attack, session establishment and resumption at the network layer; insecure interfaces, as well as insecure software, firmware, or middleware at the higher level [21].

C.2 Interoperability

In IoT systems, the interoperability issue appears on multiple levels. On the one hand, software and hardware devices must have the ability to use and exchange data or information and collaborate. On the other hand, the overall security mechanism must be standardized, and protocols implemented at various layers must interact by providing conversion methods [21]. Given the architectural constraints, especially the decentralization and heterogeneity of IoT systems, an effective combination of communication protocols and security standards at each layer is, therefore, more than necessary.

C.3 Resource Constraints

IoT devices such as sensors, actuators, and RFID tags have limited storage, computing, and battery capacity. For example, passive RFID tags have no battery and can only be powered by RFID readers or other dedicated devices. These resource constraints intuitively result in bottleneck problems when performing data access and communication operations, making IoT devices vulnerable to failure and malicious attacks [49].

C.4 Data Management

Data management entails storing, retrieving, securing, and manipulating data to ensure optimal system performance. However, most existing data management systems are built on centralized organizations like cloud-based ones. In IoT systems, centralized data management has several drawbacks that, according to Xiong et al. [49], can be identified in the following: inefficiency in terms of scalability when using centralized architectures to manage communications and data from a large number of IoT devices; confidential or private data that can be easily disclosed, modified, or deleted from a central host by unauthorized access; as well as the reliability problem caused by the presence of a single point of failure. Furthermore, having a central entity, such as an intermediary or a provider, makes practically the entire system platform-centric by granting that entity an illegal right to control and manipulate the hosted data.

IV. Blockchain

The emergence of the Blockchain offers new opportunities to overcome the IoT challenges discussed in the previous section. This section introduces the most relevant concepts and features of Blockchain technology. The idea is to go beyond the well-known use of the Blockchain for financial transactions and focus on the Blockchain-Internet of Things (BC-IoT) integration.

A. Definition

First proposed by *Satoshi Nakamoto* as the technology behind Bitcoin [31], Blockchain is a peer-to-peer network based on public-key cryptography and distributed database to establish distributed consensus among network participants without a centralized server. The Blockchain consists of a list of records called blocks (Figure 2), on which data is recorded as immutable transactions and protected by cryptographic functions, which prevent any subsequent modification [12]. A block looks like a digital container. It consists of two parts: the block header and the transactions list.

- Block header: is responsible for keeping information immutable and maintaining the link between blocks.
- Transactions list: where each transaction is a transfer of value (virtual currency, token, etc.) between two nodes in the network. It contains the sender's and the recipient's public keys and is signed with the sender's private key. Anyone on the network can use the sender's public key to check and ensure that the transaction request originates from the account owner.

B. Characteristics of the Blockchain

Blockchain is emerging today as a revolutionary technology that has many interesting characteristics, the most common of which are:

- Decentralization: is the first concept that characterizes the Blockchain, where there is no need for a third intermediary party to confirm transactions. Instead, a consensus mechanism is used to agree on the validity of the transactions.
- Transparency: data in the Blockchain is visible to everyone, allowing for more transparency in the system.
- Immutability: data in the Blockchain cannot be modified once it has been recorded. This does not imply complete immutability, but changing the data is highly difficult, and any modification is detectable.
- High availability: the Blockchain's operation relies on thousands of nodes in a P2P network where data is replicated and updated on each node. Even if some nodes leave the network or become unreachable, the system continues to work, making it highly available.
- Security and data integrity: are ensured in the Blockchain by two mechanisms: the decentralized architecture and the encryption process [42]. However, the concept of security is still a subject of debate, as all cryptographic systems have their limitations, and there is no such thing as total security. It is not only about the technology itself; it also depends on several aspects such as people, processes, networks, and usage.
- Efficiency: the Blockchain model eliminates trusted third parties or intermediaries, saving time and costs while delivering greater ease to customers.

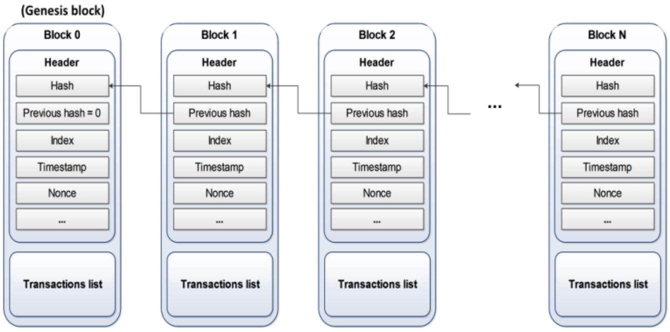


Fig. 2. Structure of the Blockchain

C. Blockchain-related Concepts

C.1 Mining

The process of adding new blocks to the Blockchain is known as mining. Nodes check if a person or an item is authorized to make a transaction and add new blocks to the chain during the mining process. Nodes could compete with each other to solve a complex computational-intensive mathematical problem such as PoW (Proof of Work) or PoS (Proof of Stake), depending on the mechanism chosen to add blocks. This process is intended to limit the possibility for malicious entities to falsify transactions [15].

C.2 Asymmetric Cryptography

Asymmetric cryptography, also known as public-key cryptography, is one of the key concepts of the Blockchain. This form of cryptography allows for verifying the integrity of transactions in the Blockchain. It uses public and private keys to encrypt and decrypt data, respectively. Standard algorithms used in asymmetric cryptography include RSA (Rivest–

Shamir–Adleman), Diffie-Hellman, ECC (Elliptic Curve Cryptography), and El-Gammal [6]. Figure 3 gives an overview of public-key cryptography.

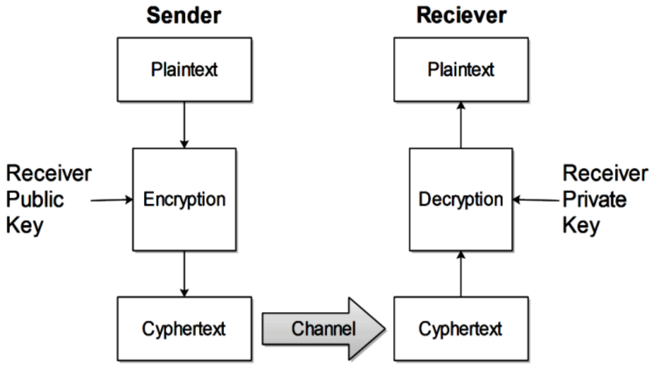


Fig. 3. Public-key cryptography scheme [6].

The sender signs data (plaintext) with his private key and generates a code (ciphertext) that is sent via the network to the receiver, as shown in the previous scheme. After it reaches the receiver, the code is validated using the sender's public key to guarantee that the data came from the sender himself. It is worth noting that the model, as it is, does not use any encryption or decryption.

C.3 Hash Functions

Hash functions are used to make fixed length digests of arbitrarily long input strings. They are keyless and ensure data integrity. MD, SHA1, SHA-2, SHA-3, RIPEMD, and Whirlpool are some of the hash functions that are commonly used in digital signatures and message authentication codes, such as HMAC (Hash-based Message Authentication Code) [6]. Hash functions have many characteristics, including:

- Compression: this attribute refers to a hash function's ability to take a large input text of any length and output a fixed-length compressed message. Hash functions generate compressed output in a variety of bit widths, typically between 128 and 512 bits.
- Easy to compute: hash functions are efficient and fast one-way functions. They must be very fast to calculate regardless of the message size. If the message is too large, the efficiency may decrease, but the function should still be fast enough for practical use.
- Pre-image resistance: for virtually any prespecified output value, it is computationally impossible to find an input that yields that value. That is, for a given y, it is difficult to find an x such that h (x) = y.
- Second pre-image resistance: it is computationally impossible to find a second entry that has the same hash value as a specified entry; for a given x, it is difficult to find a second pre-image x' ≠ x such that h (x) = h (x').
- Collision resistance: This property requires that two different input messages x and z should not hash to the same output. In other words, h(x) ≠ h(z).

C.4 Smart Contracts

A smart contract is a computer program that automatically executes and enforces an agreement between anonymous parts of the network. It contains the mutually agreed terms and conditions of transactions [6]. Smart contracts have some benefits, including:

- Autonomy and cost savings: smart contracts confirm agreements without using brokers or intermediaries, removing the possibility of third-party manipulation. Furthermore, the elimination of intermediaries results in cost savings.
- Security: smart contracts provide security by encrypting all documents and making them protected against attacks.
- Speed: smart contracts use computer protocols to automate processes, saving time for various transactions.
- Accuracy: smart contracts execute terms as they are, reducing the risk of errors or unintentional exceptions.

However, the main restriction is that it is nearly impossible to amend a smart contract; any faults in the code can be time-consuming and costly to correct.

C.5 Consensus Mechanisms

The Blockchain's backbone is the consensus mechanism. It is a set of steps followed by most or all nodes in a Blockchain network to agree on a proposed state or value. A consensus mechanism must fulfill certain criteria to deliver the desired results. These are the requirements, according to *Bachir* [6]:

- Agreement: all honest nodes choose the same value.
- Termination: once all honest nodes have completed the consensus process, a decision is made.
- Validity: all honest nodes must agree on the same value that at least one honest node proposed initially.
- Fault-tolerant: the consensus algorithm should be able to function even if one or more nodes are faulty or malicious (Byzantine nodes).
- Integrity: this is the constraint that no node can make the same choice twice in a single consensus cycle.

Blockchain consensus algorithms are the subject of much research that is outside the scope of this paper. The following list is not exhaustive, but it covers the most often used algorithms.

- Proof of Work (PoW): this consensus mechanism requires proof that adequate computational resources have been expended before proposing a value for acceptance by the network. It generally involves solving a resource-consuming cryptographic puzzle to control the generation of new blocks. This scheme is used in Bitcoin, Litecoin, and other cryptocurrencies [6]. In the IoT domain, IOTA [16] is the most prominent adopter of PoW consensus. However, PoW algorithms tend to have a high impact on battery and processing limited devices. Furthermore, PoW is most typically utilized in reward-based consensus, in which miners receive coins in exchange for their contributions to the consensus mechanism [12].

- Proof-of-Stake (PoS): is proposed as an alternative to the PoW algorithm. To reduce the difficulty of the block generation task, PoS uses a random selection of nodes based on the wealth or coinage. Although PoS aims to reduce the processing needed to create a block, to the best of our knowledge, very few studies adopt this algorithm in Blockchain-based IoT applications [13] [32]. One issue with PoS in the IoT is that it might lead to a centralization of the consensus in a few nodes, which creates a single point of attack, partially centralizes trust, and limits scalability [12].
- Practical Byzantine Fault Tolerance (PBFT): is a voting-based consensus algorithm with Byzantine fault tolerance. Even if a subset of the nodes is faulty or malicious, a distributed network can correctly reach a consensus using this algorithm. When creating a new block, a leader node is selected. This node starts the consensus mechanism by sending the block to the active nodes in the network for validation. The new block is added to the Blockchain if more than two-thirds of the active nodes vote to validate it [8]. Many Blockchain-based IoT proposals have leveraged PBFT. However, in very large networks, this mechanism may have scalability issues. Furthermore, in a dynamic P2P network where nodes leave and rejoin the networks frequently, reaching consensus becomes challenging since active nodes can change their status during consensus [12]. Various other protocols, such as DBFT (Delegated Byzantine Fault Tolerance, FBA (Federated Byzantine Agreement), Paxos [23], and Raft [33], have also been proposed for use in many Blockchain implementations.

D. *How does the Blockchain works?*

The operation of the Blockchain can be summarized in the following steps:

- Creation of the transaction: after being generated, the transaction is hashed by a hash function and associated with the issuer's private key. It is then broadcast over the network for verification and validation.
- Verification: all the network nodes can verify if the transaction is valid using the issuer's public key and a cryptographic verification algorithm.
- Creation and validation of the block: a block contains a set of transactions. It is verified and validated by the entire network. After that, it is linked to the previous blocks' chain.

V. The Integration Blockchain-IoT

As different devices and objects communicate continually to coordinate their operations and share the information they hold, the amount of data the IoT creates and has to cope with is rapidly expanding. It is now essential to have an IT infrastructure that goes beyond the current capabilities of the Internet. This infrastructure must be able to handle massive amounts of data, safe transactions, and automated value transfers [38].

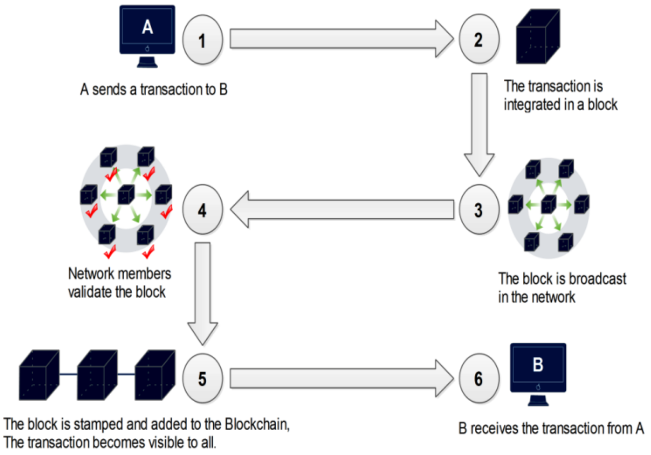

A
1
A sends a transaction to B
2
The transaction is integrated in a block
3
The block is broadcast in the network
4
Network members validate the block
5
The block is stamped and added to the Blockchain, The transaction becomes visible to all.
B
6
B receives the transaction from A

Fig. 4. Principle of the Blockchain functioning

Combining IoT and Blockchain is a very effective technique in many areas. IoT applications could benefit from Blockchain-based mechanisms to improve security, privacy, and reliability. Therefore, the Blockchain serves as a communication, access, and control platform for IoT devices. In addition, Blockchain technology reduces transaction costs and delays in IoT networks by eliminating the need for trusted intermediaries in transactions between network participants [12][38].

A. *Blockchain Implications in IoT*

Blockchain can play a significant role in facing IoT challenges. These challenges can be summarized according to the following aspects:

- Lower cost: as the number of IoT devices increases, more storage capacity is needed. Blockchain can automate the communication and the various necessary operations between the nodes of the IoT network and, at the same time, offer a permanent storage platform. As a result, the cost of Cloud-based storage, with the various maintenance and updating tasks, is significantly reduced.
- Single point of failure elimination: Cloud servers are sensitive to the single point of failure, which means that a single server's failure can affect the overall system. In the Blockchain system, all devices are connected, and all transactions are stored at each node of the Blockchain. The failure of one device will then not affect the operation of the others.
- Resistance to malicious attacks: the centralized architecture of IoT networks makes them vulnerable to many types of attacks, such as distributed denial of service, fraudulent attacks, and data theft. The distributed architecture of the Blockchain, with its chained and encrypted structure, can overcome these attacks. However, other issues can occur, such as the 51% attack.

Besides, the adoption of Blockchain technology for IoT applications has the following advantages:

- Decentralization and trust: since there is no central authority in the Blockchain, the network participants must agree on the transactions using encryption algorithms and consensus protocols, hence, ensuring trust in the network.
- Transparency: in the Blockchain, participants can view all blocks and transactions whose content is protected by a private key. Since the IoT is essentially a dynamic heterogeneous system, the transparency feature allows various devices to share their data with other devices on the network while ensuring data integrity.
- Identity management: integrating Blockchain with IoT can solve the problem of identity theft since the Blockchain has the potential to easily control and manage node identities and credentials more securely.
- Immutability: the majority of nodes have to verify any change made to the Blockchain. Therefore, transactions cannot be easily changed or deleted.
- Anonymity: to process transactions, senders and receivers use anonymous and unique address numbers to keep their identities secret. This feature is considered an advantage in some use cases, such as electronic voting.

B. Challenges and Limitations of BC-IoT Integration

Although the BC-IoT integration is promising and has many advantages, it must, however, face some challenges that can be summarized in the following [3]:

- Scalability: as the number of nodes increases, Blockchain development becomes more time-consuming and resource-intensive. One of the main challenges with BC-IoT integration is that IoT networks are expected to support a huge number of devices in diverse applications with different QoS requirements.
- Power and processing time: another challenge is the required power and processing time for all encryption operations in a Blockchain system. Several types of devices with limited capabilities exist in IoT systems, and they are unable to perform all encryption algorithms at the required speed and precision.
- Storage: in the Blockchain, there is no need for a central server to store transactions and device identifiers. But, since IoT devices typically have low storage capacity, this feature can become a constraint that slows down system operation as the Blockchain size and the number of nodes in the network increase.
- Lack of skills: Blockchain technology is still new even though there is a certain acquirement of knowledge and skills, especially in the banking and financial sector. In other areas, there is still a lack of understanding of how Blockchain works. IoT is ubiquitous but embracing Blockchain with IoT requires even more knowledge and awareness.
- Legality and compliance: Blockchain technology will connect many people and objects from different countries without complying with local laws and regulations, posing a problem for manufacturers and service providers. Also, this is a barrier to Blockchain adoption in many IoT systems and applications.

C. Existing Solutions and Trends

In light of these challenges, several solutions have been proposed, notably in terms of scalability, which is one of the most significant hurdles to Blockchain adoption. Generally, four approaches are distinguished to these solutions:

- On-chain or layer-one solutions: refer to methods working on the core elements of the Blockchain, such as blocks, consensus, and network structure. Among these methods are the SEGWIT (Segregated Witness) protocol [26] and the Sharding technique [48].
- Off-chain or second-layer solutions: these techniques offload the data from a Blockchain to the secondary channel to alleviate network congestion, reduce storage complexity, and speed up processing. Examples of Off-chain solutions include Lightning Network [35] adopted by Bitcoin, Raiden Network [37] for Ethereum, Plasma framework [36], and Cosmos [11] which is an ecosystem of Blockchains.
- Distributed ledger-based solutions: the most popular form of this approach are DAGs (Directed Acyclic Graphs), which are alternative data structures allowing asynchronous transactions processing, thereby, concurrent block generation to address speed and scalability issues with low transaction costs. IOTA, SPECTRE [44], PHANTOM [45], Byteball [10], and Nano [24] are some of the projects based on DAG.
- Consensus algorithm-based solutions: these are the various innovative consensus mechanisms that attempt to provide greater scalability and transaction processing throughput. Notable models include DPoS (Delegated Proof-of-Stake), PoA (Proof-of-Authority), and BFT (Byzantine Fault Tolerance) with its three variants: practical BFT, delegated BFT, and federated BFT [19].

While a comprehensive discussion of these approaches is beyond the scope of this paper, it is worth noting that despite their advantages, the wide range of the proposed solutions sacrifices the most fundamental property of Blockchain, namely, decentralization. Moreover, these solutions are not immune to drawbacks, some of which are summarized below:

- Most of these solutions are in the early stages of development, which raises the question of their effectiveness and reliability in facing various threats and attacks.
- Some issues relate to Sharding techniques, such as data validity and availability, transactions placement into different shards, and the efficiency of cross-shard transactions.
- Computational power and cost issues also exist in DAG-based techniques.

- In Off-chain solutions, transparency is discarded in favor of privacy; besides, there is no guarantee on data saved outside the Blockchain. For example, solutions like payment channels (Bitcoin’s Lightning Network and Raiden Network of Ethereum) are designed to process transactions off the chain, which increases the bandwidth and also the risk of data loss.
- Some issues are still open in Sharding techniques, like the placement of transactions in different shards and the efficiency of cross-shard transactions.

Interested readers are referred to [2], [19], [20], [22], and [50] for a more detailed discussion of these solutions.

VI. Proposed Approach

A Blockchain-IoT integration approach based on a layered architectural model is proposed in this section. Then, the fundamental security assumptions, and the system's functional and non-functional requirements, are defined.

A. *Architectural Model*

The architectural model consists of three layers. The first layer is the IoT network composed of different connected devices (sensors, tag readers, mobiles, etc.), whose role is to capture, collect and transmit data. The second layer is the Blockchain, composed of a set of interconnected nodes in a P2P network. The role of this layer is to validate transactions created by IoT devices at the first layer and store them permanently and immutably while maintaining their confidentiality and security. The top-level layer provides an interface for accessing and visualizing IoT data stored in the Blockchain via request/response messages, which allows for more transparency of data and information flowing over the network. Figure 5 gives an illustration of this model.

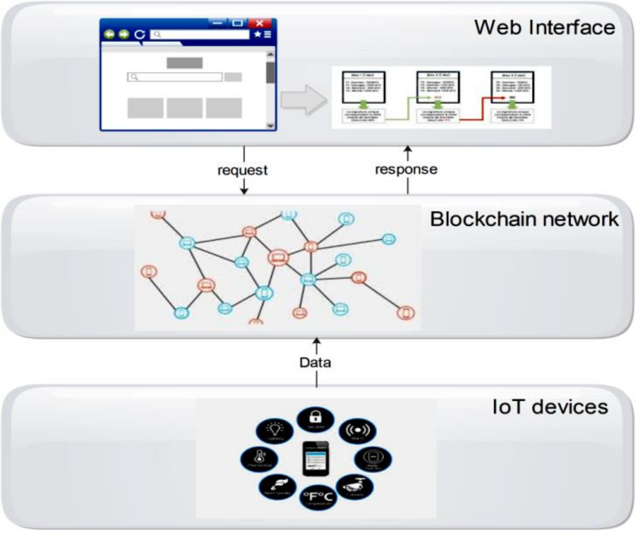


Fig. 5. The application architectural model.

It is noteworthy that the communication between the two lower layers takes place through the Publisher/Subscriber model, which consists of three components: Broker, Publisher, and Subscriber.

B. *Security Assumptions*

In the context of this work, the following security assumptions are considered:

Assumption 1: Collision resistance of hash function

This assumption is directly related to the property of resistance to collisions defined previously in sub-section (IV.C.3), where for a class of inputs I and a hash function h, if there is no polynomial-time algorithm that solves the collision problem (it means x, z ∈ I, with x ≠ z, such that $h(x) = h(z)$), then h is collision-resistant.

Assumption 2: Security of digital signature scheme

This assumption relies on the fact that for a given signature S associated with a message M and a private key Prk, if there is no polynomial-time algorithm capable of forging S for another message M' (M' ≠ M) using the public key Puk corresponding to Prk and such that the result of the verification algorithm is True, then the digital signature scheme is secure.

Assumption 3: Robustness of the Blockchain

The Blockchain's creation, including consensus and transaction addition operations, is supposed to be secure and incorruptible, ensuring tamper-proof data and event processing.

Assumption 4: Security of communication

The usage of MQTT as a communication protocol, with its basic features like authentication, access control, SSL over TCP, and WebSocket, helps to ensure a certain level of security. Furthermore, other mechanisms, such as the TLS (Transport Layer Security) protocol, which provides an encrypted pipe for MQTT messages, can be added to enhance this. MQTTS, for example, is a TLS secured version.

C. *Functional and Non-functional Requirements*

Since the requirements of such a system are highly dependent on the application domain, this section provides an identification of some functional and non-functional requirements that match with a typical IoT network use case. The functional requirements describe the processes and activities that define what the system is supposed to do or persistently provide, while the non-functional requirements define the attributes or features that specify the system's constraints and capabilities, as illustrated below.

Functional requirements:

- *Transparency:* is one of the essential factors that build trust within the network. A Blockchain-based IoT system should be verifiable and transparent to give its users the ability to have easy and reliable access to information.
- *Real-time monitoring:* the system must monitor and record all events, transactions, and object behavior throughout the network. It should also be able to satisfy real-time data processing requests.
- *Connectivity:* refers to the ability to connect devices and services using standard methods and protocols. Such a system must also offer objects the ability to use

the appropriate technology according to their constraints.

- *Identity management:* involves assigning unique identifiers to devices and transactions, enabling secure and efficient authentication and tracking of objects in the system.
- *Decentralized service:* the Blockchain-based IoT system provides a decentralized service by distributing processing and data across a peer-to-peer network. Distributed nodes, transactions, and records with validation and consensus mechanisms are used to achieve this.

Non-functional Requirements:

- *Security and privacy:* this is a big concern for IoT applications that are frequently composed of a large number of heterogeneous elements interacting in a complex environment. Thus, the system must provide a certain level of security that prevents potential threats and preserves the confidentiality and integrity of data. On the other hand, privacy-preserving, such as data anonymization during storage and communication, is also required. The usage of Blockchain will add a security and privacy layer to the IoT by using decentralization and cryptographic techniques.
- *Scalability:* this is the capacity of the system to support an increase in the number of transactions as well as the number of devices and users without deteriorating the performance and the quality of the service. Blockchain could help mitigate this issue by removing the centralization of data and treatment and enabling trust among the network without any control organization. However, scalability remains a crucial challenge that may necessitate the consideration of other aspects such as standardization.
- *Interoperability:* refers to the capacity of various IoT systems or devices to communicate and share data. A blockchain-based IoT system should be able to handle the heterogeneity of device technologies, communication protocols, and data formats.

VII. IoT-Blockchain Implementation Prototype

This section describes the realized application that implements a Blockchain for an IoT network composed mainly of mobile devices responsible for communicating the generated data to broker nodes, which are also the full nodes of the Blockchain network. Communication between IoT devices and Blockchain nodes is ensured by the MQTT protocol using HBMqtt[1] open-source library.

Table III below summarizes the scenario settings, followed by a description of the consensus mechanism used, the encryption and digital signature scheme, and the Blockchain creation algorithm.

TABLE III
Application Scenario Settings

Scenario settings	
IoT network devices	Mobiles devices
Communication protocol	MQTT
Devices identity management	public-private keys-based DID[2]
Blockchain platform type	Permissioned
Blockchain governance model	On-chain governance
Cryptographic algorithm	RSA and SHA-256
Consensus	PBFT

A. Consensus Mechanism

The PBFT consensus algorithm is used in this paper. This algorithm is simple to implement and does not require high computing resources to reach a consensus. All nodes participate in the voting process to add a new block to the Blockchain. The consensus is established if more than two-thirds of the nodes agree on this block [29][40].

B. Signature and Verification

Digital signature ensure the authenticity and integrity of data in the Blockchain. In such a system, each node has a key pair: a private key (Prk) and a public key (Puk). An algorithm A (M, Prk) is used to generate a signature S for a message M using the sender's private key Prk. On the other side, an algorithm A' (M, S, Puk) is also used to verify the signature S of message M using the public key Puk of the sender. The result of A' is True or False, thus indicating to the receiver whether the signature S is valid or not. In this paper, the RSA algorithm has been used for encryption and digital signature, where the signer holds the private key while the verifier knows only the public one**.** Figure 6 depicts this process.

C. Creation of the Blockchain

As stated above, connected objects interact with the Blockchain network via the MQTT publisher/subscriber communication model. The data generated by IoT objects are transmitted to the Blockchain through transactions. Adding a transaction is done as follows:

- Creation of the transaction and its signature with the private key of the issuer object.
- Sending the transaction to the neighboring full node (broker) using the MQTT protocol.
- Following signature verification, the transaction is grouped with others into a new block to be validated by the whole network. Once the new block is validated, the Blockchain is updated by adding this block. De facto, included transactions are confirmed.

This procedure is fundamental when adding a new block to the Blockchain, as shown in Figure 7.

The generic algorithm that creates the Blockchain is as follows:

[1] https://hbmqtt.readthedocs.io/en/latest/

[2] Decentralized Identifier

```
Input: Nodes_set: set of blockchain nodes, Pending_list: list of data not yet in the blockchain, Blocks_list : the blockchain.
    1. Generate a pair of keys for each device identified in the IoT network
    2. Get data from Pending_list and create a new transaction that contains the transmitted data along with the unique sender and receiver addresses.
    3. Generate the transaction hash with the SHA-256 function
    4. Encrypt and sign the resulted hash with the RSA algorithm
    5. Select a full node from the Nodes_set and send the signed transaction to that node for validation
    6. if the signature verification succeeds then
           Add the transaction to the new pending block
    7. Execute the PBFT consensus algorithm to verify and validate the new block
    8. if the new block is validated then
           Add it to Blocks_list
    9. for each node N in Nodes_set
           Broadcast Blocks_list
End
```

Algorithm I. Blockchain creation

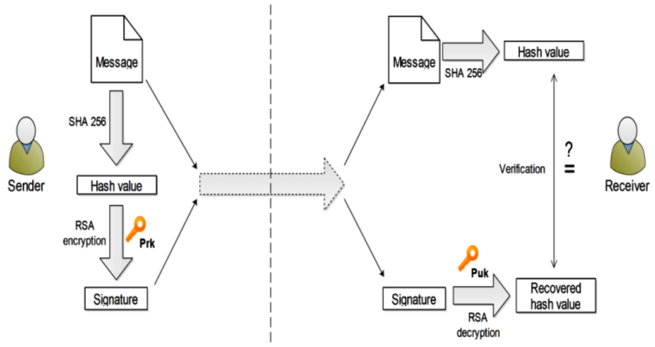


Fig. 6. Encryption and digital signature process

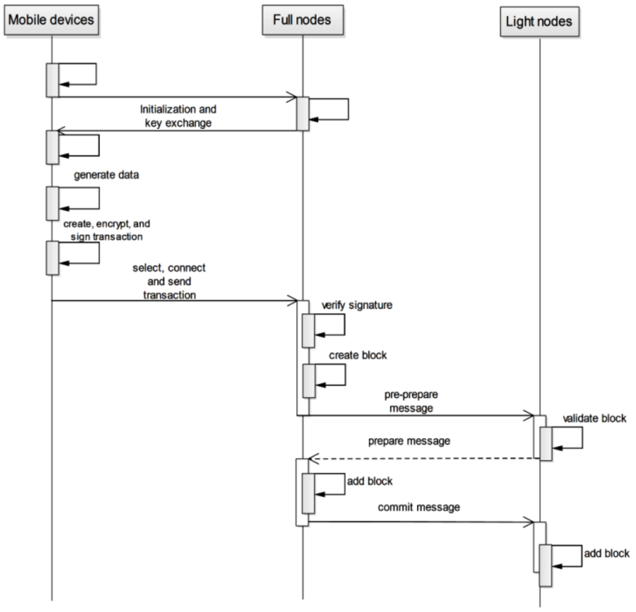


Fig.7. Sequence diagram of new block insertion

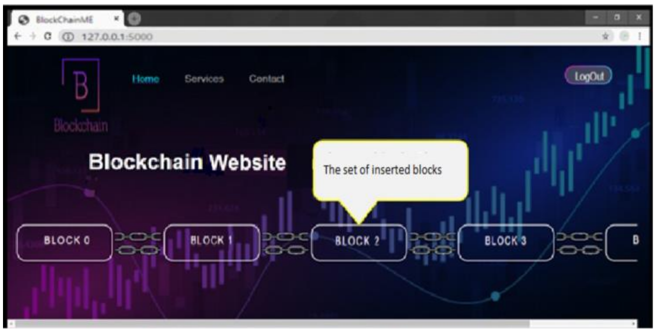
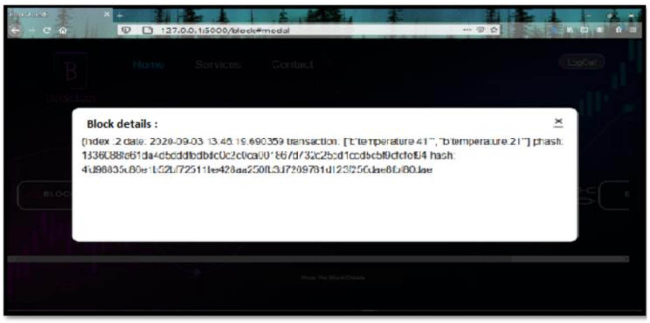


Fig. 8. Blockchain interface



Block details :

{index :2 date: 2020-09-03 13:46:19.690359 transaction: ["b'temperature:41'", "b'temperature:21'"] phash: 1336088fe61da4d5dddfbdbfc0c2c0ca00'186/d/32c25cd1ccdbcbf9dfcfof04 hash: 4d98835c80e1l52b72511be428aa250f13f7209781d123f250dae8fb80dae

Fig. 9. Example of a block content

The Blockchain is accessible through a web interface that allows the user to reach the data stored in the different blocks (Figures 8 and 9). Figure 9 shows an example of the block contents, including the block index, creation date, transaction ID, and contained data. Consequently, this makes it possible to have more visibility and transparency on the exchanges and interactions carried out at the IoT network.

VIII. CONCLUSION

The IoT is becoming more and more a very complex system that must face several challenges related to the increase in the number of connected objects on the one hand and the growing needs of users on the other hand. The diversity and heterogeneity of devices require developing solutions that ensure security, transparency, and identity management. Furthermore, centralized designs, such as cloud-based architectures, can have high overhead, latency, and potential risk of failure.

Blockchain technology, built on a peer-to-peer communication network consisting of several nodes interacting with each other without a trusted intermediary, provides a promising platform that enables IoT objects to interact reliably and securely.

After reviewing some related work in this paper, IoT and Blockchain technologies have been discussed while highlighting the concept of IoT-Blockchain integration. Then, the proposed approach, with a prototype implementation, has been detailed. The Blockchain-IoT application prototype demonstrated the capacity to store data generated by an IoT network while having a reliable and secure history of transactions and identities of objects. This prototype also allows easy access to data via a simple web interface.

Finally, as an outlook, future work will focus on:

- The scalability of the Blockchain in the face of the continuous growth of the number of connected objects. The use of lightweight cryptography is a highly recommended option in that case.

- The improvement of the consensus algorithm and its adaptation to IoT environments.

- The implementation of smart contracts in exchanging data between connected objects to make them more autonomous and interoperable.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE communications surveys & tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.

[2] A. Alrehaili, A. Namoun, and A. Tufail, "A Comparative Analysis of Scalability Issues within Blockchain-based Solutions in the Internet of Things," International Journal of Advanced Computer Science and Applications, vol. 12, no. 9, 2021.

[3] M. H. Alsharif, S. Kim, and N. Kuruoğlu, "Energy harvesting techniques for wireless sensor networks/radio-frequency identification: a review," Symmetry, vol. 11, no. 7, pp. 865, 2019.

[4] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with internet of things: Benefits, challenges, and future directions," International Journal of Intelligent Systems and Applications, vol. 10, no 6, pp. 40-48, 2018.

[5] A. Bahashwan, M. Anbar, N. Abdullah, T. Al-Hadhrami, and S. M. Hanshi, "Review on Common IoT Communication Technologies for Both Long-Range Network (LPWAN) and Short-Range Network," Advances on Smart and Soft Computing. Springer, Singapore, pp. 341-353, 2021.

[6] I. Bashir, "Mastering Blockchain," Packt Publishing Ltd, 2017.

[7] A. K. Biswal, P. Maiti, S. Bebarta, B. Sahoo, and A. K. Turuk, "Authenticating IoT devices with Blockchain," In Advanced Applications of Blockchain Technology, Singapore, 2020, pp. 177-205.

[8] M. Castro, and B. Liskov, "Practical byzantine fault tolerance," In OSDI , New Orleans, USA, 1999, pp. 173-186.

[9] B. S. Chaudhari, and M. Zennaro (ed.), "LPWAN Technologies for IoT and M2M Applications," Academic Press, 2020.

[10] A. Churyumov, "Byteball: A decentralized system for storage and transfer of value," 2016. [Online]. Available at: http://bitomer.com/byteball-web-origin/Byteball.pdf

[11] Cosmos. https://cosmos.network/, Accessed on Feb 22, 2022.

[12] V. Dedeoglu, R. Jurdak, A. Dorri, R. C. Lunardi, R. A. Michelin, A. F. Zorzo, and S. S. Kanhere, "Blockchain technologies for iot," In Advanced Applications of Blockchain Technology, Singapore, 2020, pp. 55-89.

[13] X. Fan, and Q. Chai, "Roll-DPoS: a randomized delegated proof of stake scheme for scalable Blockchain-based internet of things systems," In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York, NY, USA, 2018, pp. 482-484.

[14] M. S. Ferdous, K. Biswas, M. J. M., Chowdhury, N. Chowdhury, and V. Muthukkumarasamy, "Integrated platforms for Blockchain enablement," In Advances in Computers, vol. 115, pp. 41-72, 2019, DOI: 10.1016/bs.adcom.2019.01.001.

[15] V. Gatteschi, F. Lamberti, and C. Demartini, "Blockchain technology use cases," In Advanced Applications of Blockchain Technology, Springer, Singapore, pp. 91-114, 2020.

[16] IOTA. https://www.iota.org/, Accessed on Mar 01, 2022.

[17] D. Johnson, and M. Ketel, "IoT: Application Protocols and Security," International Journal of Computer Network & Information Security, vol. 11, no. 4, pp. 1-8, 2019, DOI: 10.5815/ijcnis.2019.04.01.

[18] G. S. Karthick, and P. B. Pankajavalli, "A review on human healthcare Internet of things: a technical perspective," SN Computer Science, vol. 1, no. 4, pp. 1-19, 2020, DOI: 10.1007/s42979-020-00205-z.

[19] G. Kaur, and C. Gandhi, "Scalability in blockchain: Challenges and solutions," In Handbook of Research on Blockchain Technology, Academic Press, pp. 373-406, 2020.

[20] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic Literature Review of Challenges in Blockchain Scalability," Applied Sciences, vol. 11, no. 20, pp. 9372, 2021.

[21] M. A. Khan, and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future generation computer systems, vol. 82, pp. 395-411, 2018.

[22] S. Kim, Y. Kwon, and S. Cho, "A survey of scalability solutions on blockchain," In 2018 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, Jeju, Korea (South) 2018, pp. 1204-1207. DOI: 10.1109/ICTC.2018.8539529.

[23] L. Lamport, "Paxos Made Simple," ACM SIGACT News (Distributed Computing Column) 32, 4 (Whole Number 121), pp. 51-58, 2001.

[24] C. LeMahieu, "Nano: A feeless distributed cryptocurrency network," vol. 4, 2018. [Online]. Available at: http://media.abnnewswire.net/media/cs/whitepaper/rpt/91948-whitepaper.pdf

[25] S. K. Lo, Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning, "Analysis of Blockchain solutions for IoT: A systematic literature review," IEEE Access, vol. 7, pp. 58822-58835, 2019, DOI: 10.1109/ACCESS.2019.2914675.

[26] E. Lombrozo, J. Lau, and P. Wuille, "BIP 141: Segregated witness (consensus layer)," GitHub, vol. 21, December, 2015.

[27] I. Mashal, O. Alsaryrah, T. Y. Chung, C. Z. Yang, W. H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68-90, 2015.

[28] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," ICT express, vol. 5, no. 1, pp. 1-7, 2019.

[29] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, and Y. Koucheryavy, "On performance of PBFT Blockchain consensus algorithm for IoT-applications with constrained devices," IEEE Access, vol. 9, pp. 80559 –80570, 2021, DOI: 10.1109/ACCESS.2021.3085405.

[30] M. H. Miraz, "Blockchain of things (BCoT): The fusion of Blockchain and IoT technologies," In Advanced Applications of Blockchain Technology, Singapore, 2020, pp. 141-159.

[31] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, pp. 21260, 2008.

[32] S. R. Niya et al., "Adaptation of Proof-of-Stake-based Blockchains for IoT Data Streams," IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019, pp. 15-16, DOI: 10.1109/BLOC.2019.8751260.

[33] D.Ongaro, and J. Ousterhout, "In search of an understandable consensus algorithm," In USENIX Annual Technical Conference (Usenix ATC 14), Philadelphia, pp. 305-319, 2014.

[34] D. Pavithran, K. Shaalan, J. N. Al-Karaki, and A. Gawanmeh, "Towards building a Blockchain framework for IoT," Cluster Computing, vol. 23, no 3, pp. 2089-2103, 2020, DOI:10.1007/s10586-020-03059-5.

[35] J. Poon, and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016. [Online]. Available at: http://lightning.network/lightning-network-paper.pdf

[36] J. Poon, and V. Buterin, "Plasma: Scalable autonomous smart contracts," *White paper*, pp. 1-47, 2017. [Online]. Available at: https://www.plasma.io/plasma-deprecated.pdf

[37] Raiden Network. https://raiden.network/, Accessed on Feb 21, 2022.

[38] P. Rathee, "Introduction to Blockchain and IoT," In Advanced Applications of Blockchain Technology, Singapore, 2020, pp. 1-14.

[39] 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.

[40] M. Salimitari, and M. Chatterjee, "A survey on consensus protocols in Blockchain for iot networks," arXiv preprint arXiv:1809.05613, 2018.

[41] S. Saxena, B. Bhushan, and M. A. Ahad, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," Journal of Network and Computer Applications, vol. 181, pp. 103050, 2021. DOI: 10.1016/j.jnca.2021.103050

[42] S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," 2016 IEEE Smart Energy Grid Engineering (SEGE), Oshawa, Canada, 2016, pp. 381-385.

[43] M. Sikimić, M. Amović, V. Vujović, B. Suknović, and D. MANJAK, "An overview of wireless technologies for IoT network," 2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH). IEEE, East Sarajevo, Bosnia and Herzegovina, pp. 1-6, 2020.

[44] Y. Sompolinsky, Y. Lewenberg and A. Zohar, "Spectre: A fast and scalable cryptocurrency protocol," Cryptology ePrint Archive, 2016.

[45] Y. Sompolinsky and A. Zohar, "Phantom," IACR Cryptology ePrint Archive, Report 2018/104, 2018.

[46] P. Thota, and Y. Kim, "Implementation and comparison of M2M protocols for Internet of Things," In : 2016 4th Intl Conf on Applied Computing and Information Technology/3rd Intl Conf on Computational Science/Intelligence and Applied Informatics/1st Intl Conf on Big Data, Cloud Computing, Data Science & Engineering (ACIT-CSII-BCD). IEEE, 2016. p. 43-48.

[47] L. Tseng, L. Wong, S. Otoum, M. Aloqaily and J. B. Othman, "Blockchain for Managing Heterogeneous Internet of Things: A Perspective Architecture," in IEEE Network, vol. 34, no. 1, pp. 16-23, January/February 2020, DOI: 10.1109/MNET.001.1900103.

[48] G. Wang, Z. J. Shi, M. Nixon and S. Han, "Sok: Sharding on blockchain," In Proceedings of the 1st ACM Conference on Advances in Financial Technologies, pp. 41-61, 2019. DOI: 10.1145/ 3318041.3355457.

[49] Z. Xiong, Y. Zhang, N. C. Luong, D. Niyato, P. Wang and N. Guizani, "The Best of Both Worlds: A General Architecture for Data Management in Blockchain-enabled Internet-of-Things," in IEEE Network, vol. 34, no. 1, pp. 166-173, January/February 2020, DOI: 10.1109/MNET.001.1900095.

[50] Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to scalability of blockchain: A survey," IEEE Access, vol. 8, pp. 16440-16455. 2020. DOI: 10.1109/ACCESS.2020.2967218.

Mansour Mededjel is an Associate Professor in the Department of Mathematics and Computer Science at the University of Ain Temouchent - Belhadj Bouchaib, Algeria. He holds a Ph.D. degree in Computer Science from the University of Oran1 - Ahmed Ben Bella, Algeria. His research interests include Internet of things, Blockchain, fog computing, physical Internet, smart logistics, and supply chain optimization.

Ghalem Belalem is a Full Professor at the Department of Computer Science in the faculty of Exact and Applied Sciences at the University of Oran1 - Ahmed Ben Bella, Algeria. He holds a Ph.D. degree in Computer Science. His current research interests are distributed system, grid computing, cloud computing, replication, consistency, fault tolerance, resource management, economic models, energy consumption, big data, IoT, mobile environment, images processing, supply chain optimisation, decision support systems, and high-performance computing.

Fatima Zohra Nesrine Benadda holds a Bachelor's degree in Computer Science, option: computer systems, and a Master's degree in Computer Science, option: networks and data engineering from the University of Ain Temouchent - Belhadj Bouchaib, Algeria.

Samah Kadakelloucha holds a Bachelor's degree in Computer Science, option: computer systems, and a Master's degree in Computer Science, option: networks and data engineering from the University of Ain Temouchent - Belhadj Bouchaib, Algeria. She is currently a software engineer in a commercial company.