International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1 (Aug-24)

http://dx.doi.org/10.12785/ijcds/160143

A Survey of Blockchain Integration with IoT: Benefits, Challenges and Future Directions

Yassine MAADALLAH[1], Nassira KASSIMI[1], Younès EL BOUZEKRI EL IDRISSI[1] and Youssef BADDI[2]

[1]*Engineering Science Laboratory, ENSA of Ibn tofail university, Kenitra, Morocco*
[2]*Department of Computer Science, EST of Sidi bennour, Chouaib Doukkali University, El Jadida, Morocco*

Received 29 Jun. 2023, Revised 7 Apr. 2024, Accepted 27 Apr. 2024, Published 1 Aug. 2024

Abstract: The Internet of Things (IoT) stands at the forefront of the latest generation of information technology advancements, signifying a crucial juncture in the integration of digital and physical domains. This integration is pivotal, facilitating a plethora of transformative digital services that substantially enhance user experiences by seamlessly melding virtual and physical elements. However, the rapid proliferation of IoT also brings to the fore a range of challenges, particularly in the realms of security, simplicity, and data integration. These challenges pose significant obstacles to the full realization of IoT's potential. This paper provides a comprehensive analysis of these challenges within the IoT framework. We delve into the intricacies of IoT environments, examining the security risks and integration complexities that arise. The paper proposes effective strategies to address these challenges, aiming to establish a more secure and reliable IoT infrastructure. We discuss innovative approaches for enhancing data integration and simplifying IoT systems while ensuring robust security measures are in place.
Through this exploration, the paper aims to contribute to the ongoing development of IoT, offering insights into overcoming its current limitations and outlining a path for its future evolution. Our analysis underscores the need for continuous research and innovation in this field, setting the stage for the emergence of more advanced, secure, and user-friendly IoT applications across various industries.

Keywords: Blockchain, Internet of Things (IoT), IoT challenges, Network security, Data privacy, consensus protocol.

1. INTRODUCTION

The emergence of the Internet of Things (IoT) marks a significant milestone in technological progress, influencing diverse sectors through its extensive network of interconnected devices. This advancement in connectivity and intelligent technology brings considerable benefits, such as increased operational efficiency, enhanced data acquisition, and widespread automation of various tasks. However, along with these advancements, the swift expansion of IoT devices also introduces a range of complex security challenges.

These challenges are a consequence of the intricate nature of IoT systems, which incorporate devices ranging from basic sensors to advanced computing units, each presenting unique vulnerabilities. As IoT finds increasing applications in critical services like healthcare, transportation, and urban management, ensuring the security of these technologies becomes crucial. This necessity is not only for the sake of efficient service delivery but also for safeguarding the privacy and security of individuals who are reliant on or interacting with these technologies.

Academic research in recent years has been increasingly focused on examining these vulnerabilities within IoT systems and evaluating blockchain's potential as a countermeasure. For instance, the work of Lo et al. [1] has shed light on the synergy between blockchain's decentralized structure and IoT's design, offering new solutions to longstanding IoT issues such as access control and data storage. Furthermore, studies by Yang et al. [2] and R. H. Weber [3] delve into the complexities of IoT security, introducing extensive frameworks and solutions tailored for IoT-based devices. These studies are instrumental in understanding the broad spectrum of IoT security, ranging from individual device vulnerabilities to network-wide risks.

Research by Aleisa and Renaud [4] has also addressed IoT privacy challenges, proposing solutions to align technological advancements with privacy rights. Similarly, Tewari and Gupta [5] have scrutinized security issues in IoT devices, underlining the evolving nature of IoT security and the need for effective protocols and privacy measures.

The role of blockchain technology in addressing IoT

E-mail address: yassine.maadallah@uit.ac.ma, kassimi.nassira@gmail.com, y.elbouzekri@gmail.com, baddi.y@ucd.ac.ma

security concerns has garnered notable interest in scholarly circles. Blockchain, characterized by its principles of decentralization, immutability, and transparency, presents an innovative approach to safeguarding IoT devices and networks. Its distributed ledger system, which records transactions across multiple nodes, offers a degree of security and trust not found in conventional centralized systems. Current research is exploring how blockchain can address specific vulnerabilities in IoT systems, such as unauthorized access and data tampering, by offering a secure and transparent mechanism for data recording and sharing. Additionally, blockchain's integration into IoT goes beyond security enhancements; it is also reshaping data management and device interoperability in IoT systems. By enabling secure and efficient data exchanges among IoT devices, blockchain technology stands to revolutionize the operational dynamics of IoT ecosystems, rendering them more resilient, self-reliant, and trustworthy. This amalgamation of blockchain and IoT presents its unique challenges and complexities, which are being actively investigated and addressed by both researchers and practitioners. Our study contributes to this burgeoning field with a comprehensive analysis of these developments, examining the opportunities and challenges of the blockchain-IoT nexus.

This paper systematically explores the intersection of blockchain technology with the Internet of Things (IoT), offering a structured narrative that spans from fundamental concepts to advanced integrations. Beginning with an introduction, the paper sets the foundation for an in-depth examination of IoT technologies, including an overview, architectural insights, and blockchain's role in surmounting IoT challenges. The subsequent sections delve into an analytical examination of blockchain, defining its core components and characteristics. The focal point of the discussion is the 'Integration and Deployment of Blockchain with IoT' section, where practical and theoretical applications are scrutinized. The paper culminates in the 'Results and Discussion' section, synthesizing key findings and insights, and then transitions to 'Future Research Directions' that envision prospective advancements. The conclusion encapsulates the study's essence, emphasizing the transformative potential and impact of blockchain within the IoT landscape.

2. INTRODUCTION TO IOT TECHNOLOGY

A. IOT OVERVIEW

Today, IoT is among the most important technologies of the 21st century. As an interconnected network, it brings together objects, services, people, and devices to perceive, collect, and transmit data via the Internet without requiring human intervention. Any object with a connection to the internet has an identity and can exchange information with other objects on the internet. Invented by smart devices with web connectivity, IoT is capable of organizing, transmitting, and reacting to any data from their respective embedded systems [6].

The IoT framework enables intelligent sensing of various information extracted from diverse applications before it is securely transmitted to the server [6].

The domain of "IoT" has greatly expanded in the last several years due to the augmentation of objects and the improvement in gadget quality, leading to financial profitability and social benefits that simplify the daily lives of individuals using this new technology [6].

B. IOT ARCHITECTURE

The structure of IoT mainly consists of three layers. Table 1 provides a detailed view of these layers, describing each layer's function and significance within the IoT architecture.

TABLE I. IoT Composite Layers

Layers	Description
IoT sensing layer	The sensing layer, often referred to as the Perception layer, forms the foundational tier in the IoT architecture. Its primary function revolves around data acquisition through a diverse array of devices, including sensors, actuators, and Internet-connected gateways. These devices work collaboratively to gather information from the physical environment, which is then relayed to the subsequent stage in the IoT framework for further processing and analysis.
Network layer	The data provided by these captures must be disseminated and stored. This task is performed by the network layer, therefore it is in charge of processing, transmitting, sending, and retrieving data, etc.
IoT software layer	These are finished products, where intelligent tasks are performed on several software. It is responsible for transmitting software resources to the client.

Note. Adapted from "Micro-Electronics and Telecommunication Engineering, Connecting Blockchain with IoT—A Review" by Anusha, R., Yousuff, M., Bhushan, B., Deepa, J., Vijayashree, J., & Jayashree, J. (2022). Singapore: Springer Nature Singapore Pte Ltd.

Recently, another layer has been introduced, known as the ”Support” or ”Middleware” layer. Situated between the connectivity and software layers, it features storage, computation, processing, and action-taking capabilities. Figure 1 below illustrates this addition to the IoT architecture.

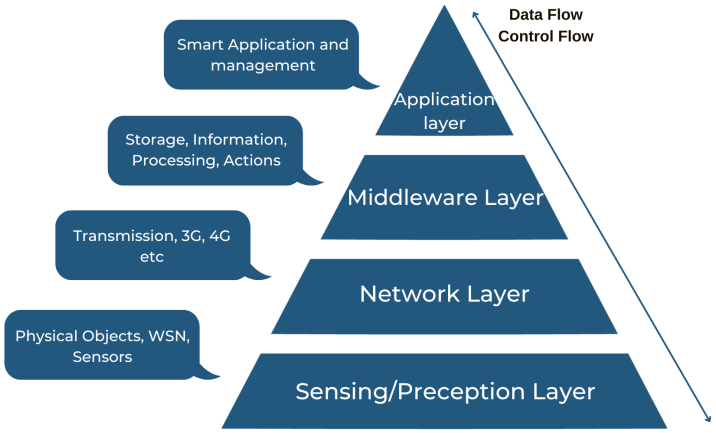

Figure 1. Architectural tiered view of IoT.

3. BLOCKCHAIN ROLES TO ADDRESS IOT CHALLENGES

Blockchain’s integration with the Internet of Things (IoT) is critical in addressing the complex challenges IoT faces in its expansive deployment across various sectors such as industry, agriculture, daily life, healthcare, IT, data analytics, and many others. The IoT, known for its rapid deployment and ease of integration with other technologies like Blockchain, Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), etc., finds a complementary ally in blockchain technology [7].

A. The challenges of IoT

The IoT, with its expansive integration across numerous sectors, has emerged as a significant boon for businesses and industries globally, offering transformative solutions and opportunities. However, alongside these advantages, IoT systems encounter a spectrum of challenges:

- **Scalability:** In today’s interconnected world, a vast network of smart devices, including phones and TVs, creates a considerable challenge in handling and processing the substantial volumes of data they generate. This necessitates advanced analytical techniques and cloud storage solutions [8]. Employing blockchain technology could provide a decentralized solution to these scalability issues. Nevertheless, blockchain also encounters its own challenges, such as restricted throughput and latency problems, which must be resolved to effectively scale it for extensive IoT applications.

- **Heterogeneity and diversity:** Product vendors aspire to introduce new services like predictive maintenance and usage billing by leveraging device connectivity and cloud-based applications. Controlling the heterogeneity of their device portfolio in the Internet of Things remains a significant challenge [9]. Blockchain can play a role in standardizing communication protocols and data formats, thereby reducing complexity.

- **Privacy, confidentiality and data integrity:** With the massive user base for IoT, data traverses many network hops, necessitating encryption to maintain confidentiality and prevent unauthorized access [10]. Blockchain technology can enhance data integrity and privacy through its cryptographic mechanisms. However, the transparent nature of blockchain poses challenges to user anonymity and data privacy, which need innovative solutions such as zero-knowledge proofs or private transactions.

- **Security:** Security remains a critical aspect of IoT, with the nature of risks varying across its different layers [11].
  Conventional methods such as authentication and encryption might not always be practical for IoT systems constrained by resources [12]. Additionally, the issue of delayed security firmware updates further exacerbates IoT’s susceptibility to cyber threats. While blockchain technology enhances security through a tamper-proof ledger for transaction recording, securing the blockchain itself, particularly in public networks, poses its own set of challenges.

- **Immutability:** Regarding immutability, changes within the network can create security and privacy complications [13].Blockchain technology provides a ledger that is immutable, which is advantageous for ensuring auditability and fostering trust. Nonetheless, this characteristic of immutability can be problematic, particularly when there’s a need to correct or remove data. This situation underscores the necessity for blockchain solutions that are adaptable and can accommodate such needs.

In summary, blockchain technology presents promising avenues to address the challenges in IoT, but it also brings its own set of challenges, particularly in scalability, privacy, and anonymity. These require careful consideration and innovative solutions to fully leverage blockchain’s potential in the IoT domain.

B. IoT classifications

There are different types of IoT applications depending on their use. Here are the different categories of IoT, based on the customer base and device usage:

- **Consumer IoT:** This is the everyday use of the Internet of Things, where users use devices such as smart TVs, intelligent cars, smartphones, smartwatches, laptops, connected devices and entertainment systems for

personal use [14].

- **Commercial IoT:** Commercial IoT goes a step further, offering the benefits of IoT outside the home. Includes such things as personal control schedules, building access, as well as connected lighting, asset tracking, and many other things [14].
- **Industrial IoT:** These are the automated systems that aim to improve existing industrial systems, and make them both more productive and more efficient.
  These include connected electricity meters, weather or traffic monitoring systems, water quality monitoring systems, smart lighting and security systems, and many others [14].
- **Internet of Military Things:** Mainly related to the military domain. It is primarily aimed at increasing situational awareness, improving risk assessment and improving response times [15].
  Common IoT applications include connecting surveillance robots, wearable biometric systems for combat, aircraft, tanks, soldiers and even drones via an interconnected system.

These categories are further illustrated in Figure 2, providing a visual representation of the different types of IoT applications.

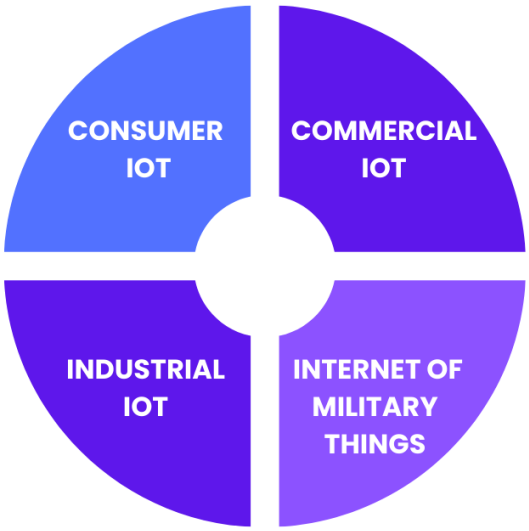

Figure 2. Types of IoT Devices.

C. The role of blockchain in the IoT technology

Modern IoT systems consist of an extensive array of devices, objects, and numerous sensors, all interlinked to facilitate a variety of operations within an IoT setting. Managing and overseeing this vast network of devices presents significant complexity. The prevalent use of centralized servers for data storage, authentication, and analysis introduces heightened risks of network attacks [16].

Blockchain technology emerges as a vital solution to address the privacy and security challenges inherent in IoT systems. The utilization of smart contracts in blockchain plays a crucial role in the management and security of IoT devices, offering a more robust and decentralized approach to protecting these interconnected systems [16].

The benefits of combining blockchain with IoT are numerous, as depicted in Figure 3 below. These benefits include improved data privacy and security, enhanced transparency, and the elimination of centralized authority, which is pivotal in addressing many of IoT's inherent challenges.

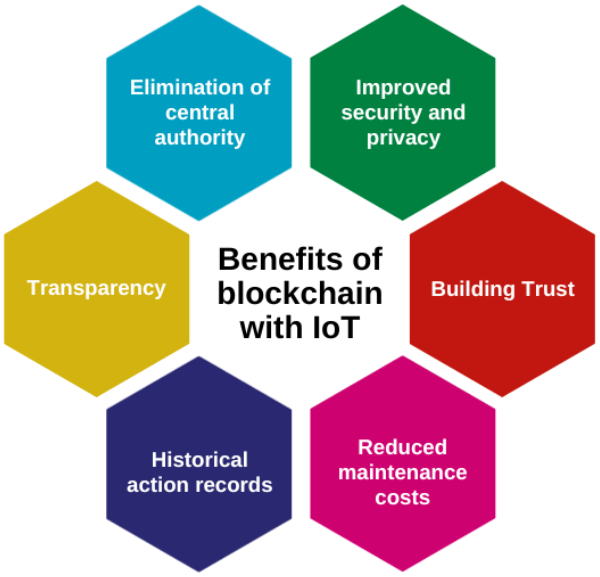

Figure 3. Benefits of IoT blockchain integration

- **Elimination of central authority:** Blockchain technology, due to its decentralized nature, eliminates the concept of centralized servers. To effectively solve bottlenecks and failures from a single point by removing the necessity of a reliable intermediary in the IoT, blockchain is the ideal solution. A decentralized storage of data where every participant in the network maintains a record of all transactions. Thus, mirror copies of constantly updated data will reside in the network nodes rather than in centralized nodes. So by integrating Blockchain into at every tier of the IoT framework, whether it's edge servers or cloud servers, we create decentralized database storage. This will avoid redundancies and make disruptions very complicated [16].
- **Improved security and privacy:** Ensuring robust network security stands as a critical challenge in the realm of IoT. Blockchain technology emerges as an optimal solution to ensure data confidentiality and security. It achieves this by storing data as encrypted transactions, which are digitally signed using encryption keys. Furthermore, the implementation of

smart contracts in blockchain could offer advanced solutions for reinforcing IoT system safety. This includes the autonomous upgrading of IoT device firmware, adding an additional layer of security to these interconnected systems [12].

- **Building Trust:** Greater trust in IoT data can be achieved by ensuring that mechanisms are in place to prevent data from being altered or falsified. This is what blockchain technology enables, thanks to its peer-to-peer network using a consensus algorithm, where all participants have an unforgeable record of all transactions [16].

- **Historical action records:** All transactions made through the IoT are stored in the blockchain and are verifiable and identifiable anywhere, anytime, by any participant in the network, all the way back to the origin of the transaction (the first transaction) [12]. The traceability functionality provided by the blockchain guarantees the improvement of the quality of service and the reliability of IoT data, as it allows the traceability of resources and the verification of the agreement that describes the level of service expected by customers from their IoT service providers, on the one hand, and on the other hand, it guarantees that the transactions stored in the blockchains have no possibility of being altered or modified [12].

- **Transparency:** In IoT systems, users often lack visibility into the use and management of their data, presenting a significant transparency challenge. Blockchain technology offers a compelling solution to this issue. It ensures that data is not only more transparent but also more accurate than in traditional networks. This transparency is crucial for maintaining the integrity and trustworthiness of blockchain-based systems, as it reduces the risk of unauthorized data modification. The immutable nature of blockchain, which mandates network-wide consensus for altering any transaction, empowers all users with equal rights to observe and verify transactional activities. This consensus mechanism enhances the transparency and reliability of the entire network, thereby addressing one of the critical challenges in IoT systems. [17].

- **Reduced Cost:** Cost reduction is one of the main objectives of many companies. This step is very important as it consists of finding efficient and economical methods to process the massive volume of data generated by IoT sensors.
Although centralized cloud storage services offer much lower prices for storage and computation, blockchain can further reduce these costs by significantly reducing the cost of maintaining dedicated servers, without obliterating the role of blockchain that also avoids the cost of third-party services.

4. OVERVIEW OF THE BLOCKCHAIN

A. DEFINITION OF BLOCKCHAIN

Blockchain technology is conceptualized as a collaborative ledger, crucial for recording data generated across a network by various participants. It functions as a distributed database, where user-contributed data is immutably stored as a public ledger in a decentralized setting [18].

This technology comprises a series of interconnected blocks, forming a chain. Each block contains a timestamp and transaction data, secured using public key cryptography. The integration of encryption methodologies, secure digital signatures, and a distributed consensus algorithm renders the blockchain both decentralized and reliable

An illustrative representation of blockchain's structure is shown in Figure 4. This figure provides a visual breakdown of the blockchain components, illustrating how individual blocks are linked together and the nature of the information each block typically contains.

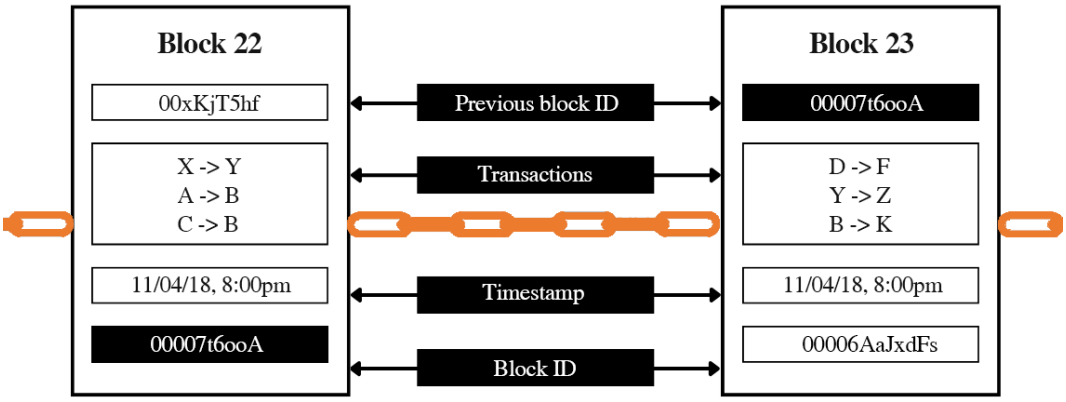

Figure 4. The structure of a blockchain [19]

Each transaction is distributed and authorized on a P2P network, each participant in the network confirms and validates the protected transaction message, while each member of the network receives the updated copy of the

ledger to be able to verify new transactions, and once the transaction is executed and recorded, it is inserted sequentially and in chronological order into the chain, and can neither be modified nor reversed [20]. This is what makes the blockchain an indelible historical registry by making a transparent record of every transaction. Figure 4 represents the structure of blocks in the Distributed ledger system (Blockchain system).

B. BLOCKCHAIN COMPONENTS

Blockchain technology is built upon several key concepts, including transactions and blocks. This section delves into these fundamental components, explaining their roles and functionalities within the blockchain system.

1) The block

At its core, a blockchain is a chain of blocks, each serving as a repository for a set of data. This characteristic underlines the block's status as the foundational element for the functioning of a blockchain. Conceptually, each block can be likened to a page in a ledger. It serves as a record in the blockchain, capturing and validating multiple pending transactions or data entries.

A block is composed of various attributes and details that define its structure:

a) Block header:

The block header is a crucial component of a blockchain block, encompassing several key elements that are essential for the block's functionality and identity within the blockchain [6]. To provide a clearer understanding of these elements and their arrangement, Figure 5 is included. This figure visually details the structure and format of data blocks within a blockchain.

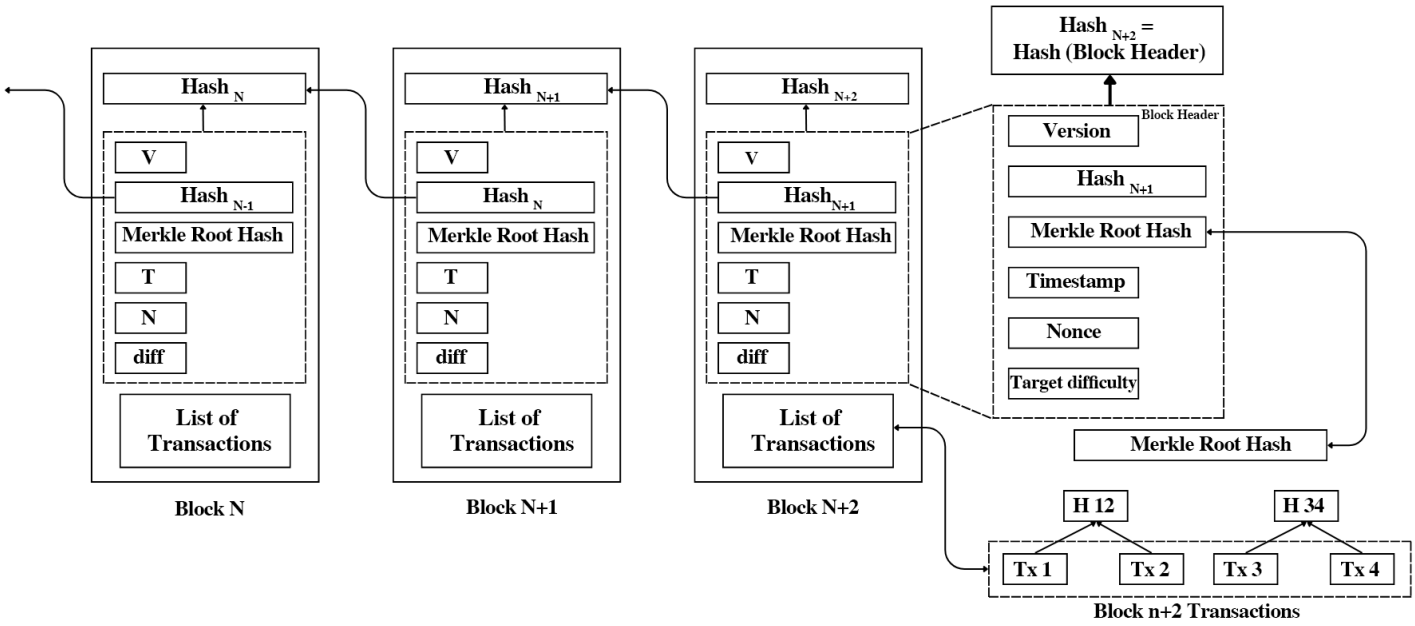

Figure 5. Structure and Format of Data Blocks in Blockchain [21]

- **The version of the block:** It is in fact necessary to mention all the rules of validation of the blocks that will be used.
  It is important for the right reading of the information in each block.
- **Hash of parent block:** Each block reference to the preceding block, called the parent block, is made by embedding the hash of the previous block in a specific field of its header. This essentially means that every block has the hash of its parent in its header, which affects its own hash.
- **Merkle root hash:** It indicates the total number saved during the duration of the transaction in the block hash value.
- **Timestamp:** Each block in the blockchain system includes includes a timestamp called a Unix timestamp at which time it was extracted.
- **Nonce:** It is a 32-bit field that usually starts with zero (0) and is augmented with each hash computation.
- **nBits:** A brief description of the actual hash target.
- **Number of transactions:** Represents the overall volume of transactions contained in this block. Figure 5 provides a detailed view of a block.

b) Block body:

The body of each block includes a transaction counter. In addition, the complete tally of transactions that a block

has is defined by the block size and the transactional data volume [7].

2) Nodes

Each node in the decentralized network is responsible for storing a copy of the transaction on the network, in addition to the possibility of playing effective roles represented in performing important functions such as verifying and authenticating transactions.

With the specific role of a blockchain node, it is possible to use it to :

- Confirm or decline the transaction.
- To verify and manage a transaction.
- Store and encrypt blockchain data.

Since it is a decentralized distributed P2P network, any number of nodes can interact with each other without the need for a central authority. A node is generally a device like a mobile phone, a server or a mobile phone, or a computer connected to the blockchain network, which represents a particular user.

Different types of nodes can be found in blockchain networks. It contains full nodes, light nodes, super nodes and lightning nodes. A brief review of two of the more important types of nodes is provided below:

a) Full nodes:

A full node contains the complete history of all transactions made on the platform from the first transaction to the current transaction, a full node has specific responsibilities such as verifying all transactions and maintaining consensus among other nodes that distinguish it from other nodes in the network. Full nodes follow and adhere to all the rules of the consensus algorithm for adding blocks to the network.

b) Light nodes:

Light nodes contain light or limited information. These nodes do not necessitate the storage of a full copy of the blockchain, where we find that the light nodes contain only the information of the previous block they are linked to, and this information is stored and saved in the block header.

These light nodes for network access always rely on a third party acting as an intermediary. They rely on full nodes to provide them with information such as account balances and recent header requests.

Because these nodes do not demand a high disk space and resources to function due to their light weight. A light node can be run on mobile devices such as phones and tablets, as 200 MB of disk space and some processing power is sufficient to run it.

3) Transactions and digital signatures

In a blockchain network, transactions, whether they involve cryptocurrency or simple data exchanges, are facilitated by peers using a public-private key pair. The private key enables peers to sign transactions digitally. These transactions are directed to the recipient's address on the blockchain, which is derived by computing the cryptographic hash of the sender's public key [22].

For instance, in Bitcoin's blockchain, SHA-256 encryption is used to generate user addresses. This process effectively masks the transparency of the public keys in cryptocurrency applications. In these networks, tokens are not sequentially distributed; rather, a specific number of tokens are initially linked to addresses in the early blocks of the blockchain. Transactions monitor token ownership by adjusting the number of tokens associated with each address involved in transactions outside the realm of cryptocurrency. It's important to note that transactions themselves do not define token ownership. Instead, they rely on the secure exchange of data, which is safeguarded by digital signatures [22].

Figure 6 illustrates a Bitcoin blockchain transaction, emphasizing the importance of digital signatures and cryptography for security.

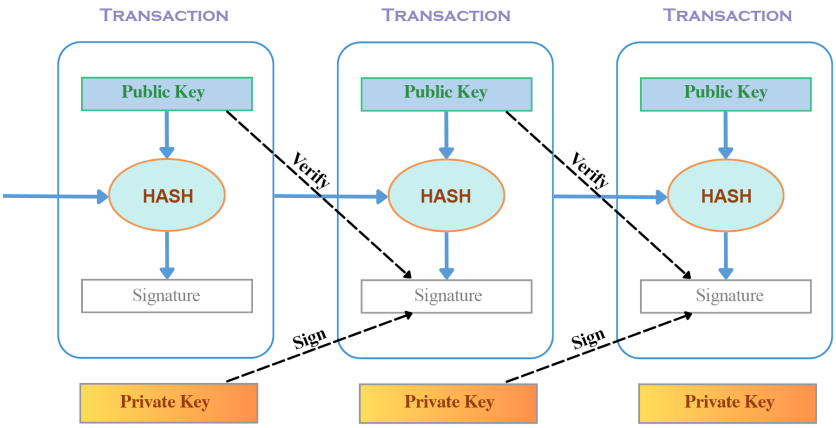

Figure 6. Architecture of a Bitcoin Blockchain Transaction [23]

In this example, we use Alice's situation to demonstrate how blockchain transactions are executed, specifically in scenarios lacking encryption. Alice initiates the process by encrypting the transaction information with her public key and then sends a portion of it to Bob. Next, she computes a hash of the transmitted data and secures it using her private key, thus forming a cryptographic signature. Each transaction is comprised of this encrypted information as well as the digital signature, both incorporated into the header of the transaction. The transaction is then disseminated across the distributed ledger network. Since the transaction is directed to Bob, he needs to use Alice's public key to decrypt the digital signature and verify the transaction details. Then, he uses his own private key to decrypt the actual data. This procedure is noted for its ease and clarity, particularly due to the comparison of the data hash against the digital signature[22].

4) Consensus algorithm

At the moment where the transaction is to be integrated into the network of successive blocks, it must be validated and verified after acceptance by all nodes in the network in a process called the consensus algorithm (CA).

Consensus allows all nodes to operate in a P2P network collaboratively without the need to know or trust each other. This consensus protocol is designed to allow the blockchain to be updated securely by following specific rules, which control the entire operation of the network and all of its core components [24].

These rules apply to how to add a block, how to determine if a block is valid and how to resolve validity conflicts. In the case of IoT, the consensus algorithms applied must meet several needs and requirements such as security, energy consumption, in addition to certain computing requirements [24].

Below we present some consensus mechanisms explained in a simplified manner and discuss their viability in IoT solutions.

a) Proof-of-Work (PoW)

Currently, the most recognized consensus mechanism in blockchain technology is Proof-of-Work (PoW), notably utilized in Bitcoin's blockchain system.

At the core of the PoW protocol is the principle that any network node can contribute to the generation of new blocks by undertaking computationally intensive tasks. This process of creating new blocks within the PoW framework is commonly referred to as "mining." In this context, miners, who are the active nodes in the network, receive rewards in the form of bitcoins, and occasionally, transaction fees, in return for their computational efforts [24].

From a network security perspective, the majority of the blocks are added to the longest chain by miners, owing to its established reliability. The PoW mechanism remains secure as long as no single entity controls more than 51% of the total computational power of the network, ensuring that the majority of the mining power resides with legitimate participants [24].

b) Proof-of-Stake (PoS)

According to the principle adopted by Proof of Stake, the more value you have in play in the system, the lower the incentive to create a malicious block [6]. Users are therefore encouraged to indicate that they have a large number of crypto-currencies.

PoS uses a validation process based on peercoin and blackcoin, in peercoin the old coins have a better chance of mining the next block, but blackcoin is based on randomness [13].

The advantage of using PoS in the place of PoW is the cost effectiveness because it uses much less energy so Pos would be a good solution for IoT. With PoS a possible disadvantage is that always the node that has a number of value has more control over the network [24].

c) Proof of activity

Has been proposed as similar to PoW, it provides a consensus that is used to ensure that all transactions performed on the blockchain are genuine, proof of activity is a hybrid approach that merges the two most used algorithms PoW and PoS and tries to provide the best of both [22].

Proof of activity involves miners generating a new block that includes header information and the miners' payment address to successfully resolve a cryptographic computation. After finding a new block, a PoS validation randomly chooses a group of block validators (hashers or miners) based on their participation in the currency. The probability for validators to be selected is proportional to their share in the network is similar to that of PoW, once the validation is completed, the block will be published [22].

Proof of activity is not a good choice for IoT applications because it requires higher computational power and suffers from the same shortcomings as PoW.

d) Proof of Elapsed Time (PoET)

Developed by Intel for the Hyperledger Sawtooth Blockchain project, the Proof of Elapsed Time (PoET) presents a distinct approach to blockchain consensus algorithms [25]. This method marks a departure from the traditional consensus mechanisms previously discussed.

In PoET, before the creation of a new block, each participating node receives a randomly assigned wait time. The node with the minimum waiting period becomes the validator responsible for mining the next block. This process is facilitated by the trusted platform Software Guard Extensions (SGX) [17].

PoET stands out for its energy efficiency, particularly when compared to other consensus algorithms like Proof of Stake (PoS) and Proof of Work (PoW). It eliminates the need for high-end, power-intensive hardware or substantial computational resources. Given these characteristics, Proof

of Elapsed Time emerges as a compelling and energy-efficient solution for private IoT blockchains.

5) Smart contract

Smart contracts, a concept introduced in the 1990s, are essentially programmable applications designed to facilitate monetary transactions and store critical data on the blockchain under predefined conditions [13]. These contracts are executed automatically when the specified conditions are met, eliminating the need for intermediaries. They are envisaged to replace traditional contracts, offering a more efficient and secure method of enforcing agreements.

In the realm of IoT, smart contracts open up new possibilities. They enable IoT devices to automate actions based on pre-agreed terms, enhancing the functionality and potential applications of IoT solutions [24]. This automation and self-execution of contracts have significant implications for various industries, streamlining processes and ensuring the integrity and reliability of transactions.

To illustrate how smart contracts function within the blockchain framework, Figure 7 provides a diagrammatic representation. This figure explains the operational mechanism of smart contracts, showcasing the automated process that gets triggered under specific conditions set within the contract.

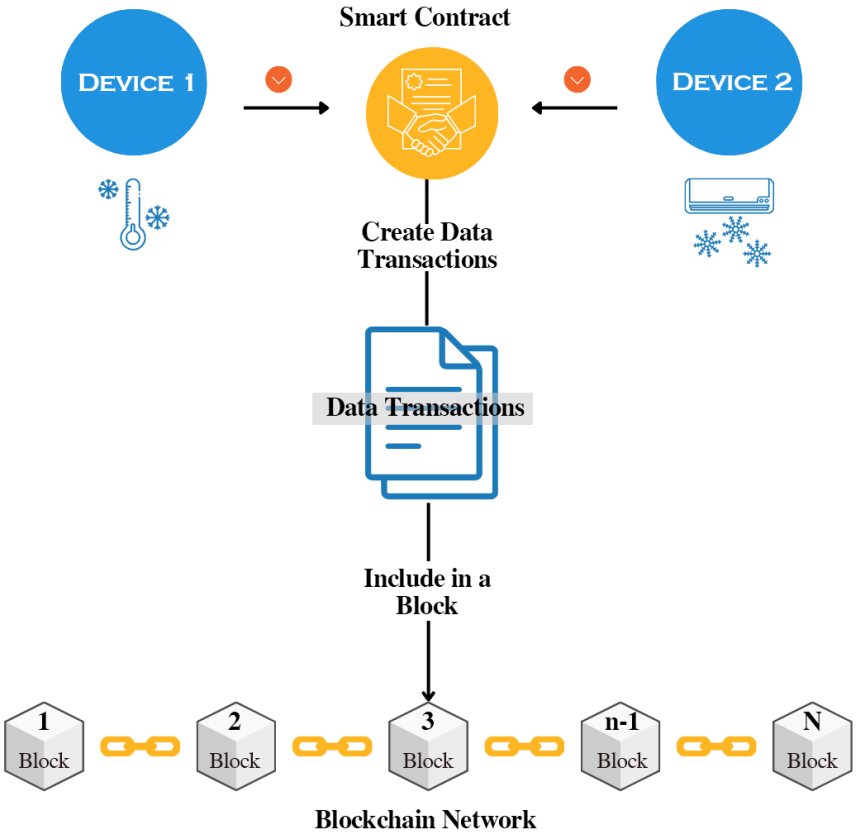

Figure 7. Diagram showing how a smart contract works [26]

5. TAXONOMIES AND KEY CHARACTERISTICS OF BLOCKCHAIN

A. BLOCKCHAIN KEY CHARACTERISTICS

This section describes the characteristics that differentiate blockchain technology, which gives a strong added value and quality to all areas that use blockchain technology.

- **Immutability:** The structure of a blockchain comprises a series of blocks, each linked to the preceding one through a reverse hash reference. Concurrently, the root hash of the Merkle tree encapsulates the hash of all the constituent transactions. Alterations in any transaction lead to the generation of a new Merkle root, enabling the immediate detection of potential fraudulent activities. This integration of diverse hash references with the Merkle tree structure serves as a robust mechanism to ensure the accuracy and integrity of information within the blockchain [8].

- **Decentralization:** In classical decentralized transactional systems, the approval of transactions is performed by a reference organization, which necessarily requires implementation traffic and expensive overhead on the central servers. In contrast, the blockchain allows transactions to be validated without control from a central authority [8].

- **Traceability:** The blockchain includes the history of all transactions since the date of its creation. Any transaction stored in the blockchain is time-stamped. Every user can easily verify and follow the starting point of information of historical data as a soon as the information of the blockchain is analyzed with the corresponding timestamps [16].
- **Pseudonymity:** A level of protection can be preserved in blockchain systems by anonymizing the addresses of the blockchain to ensure privacy. The blockchain can preserve only pseudonymity instead of complete confidentiality to allow the blockchain information to help identify scams and illegal transactions [8].
- **Non-repudiation:** Within blockchain technology, a transaction is appended with a signature using the initiator's private key. This signature is then accessible and verifiable by other network participants through the matching public key. As a result, a transaction that has been cryptographically signed is irrefutable, ensuring that the originator cannot deny initiating the transaction [12].
- **Transparency:** The information encapsulated in the blocks is transparent to all participants who have the ability to access and verify the transactions committed to the blockchain [16].
- **Persistence:** Transactions are often validated fairly quickly and invalid transactions would not be accepted by honest miners. Once a transaction is incorporated into the blockchain, it will be almost impossible to remove it [7].

B. TAXONOMY OF BLOCKCHAIN SYSTEMS

- Public blockchain: It is a new distributed ledger technology with no restrictions or permissions, where every member of the blockchain network can contribute to the distribution of new blocks and the use of blockchain content [27].
- Private blockchain: Appropriate for companies operating in a restricted environment under a structured administration where only certain members can join the blockchain network. [27].
- The consortium blockchain is used as a hightly reliable, audited, and coordinated distributed database that ensures the exchange of data between the various consortium parties contributing to the project. Consortium blockchain brings together multiple organizations and serves to maintain transparency between the parties involved in the network [7].

Table 2 presents a comparison of blockchain types.

TABLE II. Comparative Analysis of Different Blockchain Variants

Defining Features	Public Blockchain	Private Blockchain	Consortium Blockchain
Scalability	Limited	High	Moderate
Decentralization	Fully Decentralized	Centrally Controlled	Semi-Decentralized
Flexibility	Limited	High	Moderate
Consensus	PoW, PoS	Ripple Consensus Mechanism	PBFT, PoA, PoET
Transparency	High	Low	Partial
Traceability	Completely Traceable	Wholly Traceable	Traceable to an Extent
Immutability	Completely Immutable	Modifiable	Partially Immutable

Note. Adapted from "A Survey on Blockchain for Industrial Internet of Things" by Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2022). Alexandria Engineering Journal, 61(8), 6001–6022. Copyright 2022 by Elsevier B.V.

6. INTEGRATION AND DEPLOYMENT OF BLOCKCHAIN WITH IOT

This segment provides an extensive review of practical implementations and scenarios that demonstrate the fusion of blockchain technology within the Internet of Things (IoT) across diverse industrial fields. These real-world examples highlight the effectiveness of integrating blockchain into IoT systems, emphasizing its contribution to reducing security vulnerabilities and driving significant innovation. Each example detailed reinforces blockchain's capacity to enhance data veracity, openness, and reliability in IoT frameworks.

A. REAL-WORLD EXAMPLES AND USE CASES

The burgeoning synergy between blockchain and the Internet of Things (IoT) is progressively transcending theoretical boundaries, manifesting in varied and impactful real-world applications. This section aims to elucidate the practical manifestations of this convergence across diverse sectors, thereby substantiating the theoretical underpinnings of blockchain technology with empirical examples.

In this exploration, we systematically dissect select use cases spanning sectors such as supply chain management, healthcare, urban infrastructure, industrial IoT, domestic IoT applications, and the automotive industry. Each case study is meticulously chosen to exemplify the unique applications of blockchain in conjunction with IoT technologies, underscoring transformative solutions that significantly elevate operational efficiency, security, and trustworthiness.

Our analysis not only highlights the successful deployment of these technologies but also critically examines the challenges and limitations encountered during their implementation. This balanced approach is intended to present a realistic perspective, acknowledging the intricacies inherent in the integration of these advanced technologies.

Through this comprehensive overview, the section endeavors to offer an in-depth understanding of the collaborative impact of blockchain and IoT across various industries. This synthesis aims to paint a picture of a future where these technologies collectively foster a more interconnected, secure, and efficient global landscape.

- **Blockchain in Supply Chain Management:** In the realm of supply chain management, the integration of blockchain technology has emerged as a pivotal innovation, particularly in enhancing security and traceability. The paper by Author et al. [28] presents a compelling case for this integration, focusing on the augmentation of food supply chain security through the use of blockchain and TinyML. This study underscores the significance of blockchain in ensuring the integrity and transparency of supply chain processes, a critical factor in industries where authenticity and quality control are paramount. By leveraging blockchain's decentralized and immutable ledger system, stakeholders in the supply chain, ranging from producers to consumers, benefit from an enhanced level of trust and verification capabilities. Furthermore, the integration of TinyML with blockchain in this context illustrates an innovative approach to addressing complex challenges such as food fraud, contamination, and supply chain inefficiencies. This example not only demonstrates the practical application of blockchain in supply chain management but also highlights its potential to revolutionize the sector by introducing new levels of efficiency, accuracy, and trust.
  In addressing scalability, this case study demonstrates the use of blockchain in managing large volumes of data across the supply chain, showcasing how blockchain technology scales to accommodate extensive networks of suppliers and consumers. However, challenges remain in ensuring high transaction speeds and handling large data volumes in real-time.

- **Blockchain in Healthcare:** In the healthcare sector, the convergence of blockchain technology with the Metaverse and AI is revolutionizing patient care and data security. The paper by Ali et al. [29] delves into this integration, illustrating a novel architecture that empowers immersive patient care while fortifying trust and security through blockchain. This architecture, facilitating virtual healthcare interactions, leverages blockchain's attributes of transparency and immutability to safeguard patient data and ensure privacy. The study illuminates the transformative potential of blockchain in healthcare, particularly in enhancing patient experiences within the Metaverse. It underscores blockchain's role in managing sensitive health data, mitigating privacy concerns, and providing a secure environment for virtual consultations and treatments. By incorporating blockchain, the healthcare Metaverse achieves a new paradigm of trust and security, addressing critical challenges faced in virtual healthcare delivery and patient data management.
  The integration of blockchain in healthcare, as demonstrated in this study, places a significant emphasis on privacy. The use of blockchain ensures that patient data remains secure and private, addressing concerns about unauthorized access and data breaches. Yet, the challenge of maintaining patient anonymity within the transparent blockchain network requires further innovative solutions.

- **Blockchain for Smart Cities and IoT Utilities:** In the evolving landscape of smart cities, the Internet of Things (IoT) plays a transformative role, as elucidated in the comprehensive study by Rejeb et al. [30]. Their bibliometric analysis of 1802 articles reveals a significant growth in IoT research, particularly in its integration with technologies like cloud computing, big data analytics, blockchain, and artificial intelligence. Smart cities, defined as technologically advanced urban areas harnessing ICT and IoT for improved operational efficiencies and quality of life, are rapidly adopting IoT for its ability to interconnect various city services and infrastructure. This integration optimizes services such as transportation, healthcare, and urban management, simultaneously addressing challenges like security, privacy, and data integrity. Blockchain technology, in this context, emerges as a critical component in ensuring the security and privacy of IoT-based smart city applications. The combination of IoT and blockchain in smart cities not only facilitates seamless and secure communication among diverse and interconnected devices but also addresses the intrinsic challenges of IoT implementation, including heterogeneity, data privacy, and regulatory uncertainties.
  In this context, blockchain technology addresses the challenge of scalability by enabling efficient and secure communication across the myriad of interconnected devices within a smart city. Privacy and data integrity are also key considerations, with blockchain providing a secure framework for data exchange. However, ensuring user anonymity in such a widespread and interconnected system remains a complex issue.

- **Blockchain in Industrial IoT (IIoT):** In the sphere of Industrial Internet of Things (IIoT), the enhancement of smart factory performance through automation and scalable functions is increasingly pivotal. The research by Manogaran et al. [31] introduces a

novel blockchain-assisted secure data sharing (BSDS) model, aimed at optimizing industrial automation in terms of sharing, security, and scalability. This model uniquely amalgamates blockchain technology with intelligent computing and machine learning methods to analyze and secure the communication between devices in smart industries. The BSDS model's primary design goal is to augment the reliability of data handling, effectively mitigating security threats and false alarm progressions in the IoT-driven industrial environment. By ensuring secure data gathering and dissemination across various levels of smart industry infrastructure, this model significantly improves the overall performance of smart factories and industries, safeguarding against data forging attacks and enhancing operational efficiency. The implementation of this model illustrates the transformative potential of blockchain in IIoT, particularly in reinforcing security measures and streamlining data exchange processes.
In terms of scalability, the BSDS model showcases blockchain's ability to efficiently manage large-scale data sharing and communication in industrial environments, demonstrating how blockchain scales effectively in IIoT settings. However, the continuous expansion of IIoT systems presents ongoing scalability challenges that require innovative blockchain solutions to accommodate growing numbers of interconnected devices. In addressing privacy and anonymity, the model leverages blockchain's secure framework, yet the challenge remains to balance transparency and privacy in such environments, especially when handling sensitive industrial data.

- **Blockchain Applications in Smart Home Environments:** Within the smart home sector, the adoption of blockchain technology is becoming crucial to strengthen security and privacy. This importance is accentuated by the extensive reach of IoT frameworks. Farooq et al. [32] have developed an innovative architecture for a private blockchain-based smart home network, utilizing a cutting-edge Fused Real-Time Sequential Deep Extreme Learning Machine (RTS-DELM) system. This method significantly reinforces smart home security by facilitating the precise identification and thwarting of unauthorized actions. The technique utilizes fusion processes at both the data and decision-making levels to enhance the accuracy and dependability of intrusion detection in smart home networks. Their research demonstrates how such a sophisticated methodology refines smart home networks, improving their capability for effective surveillance and safeguarding against detrimental or intrusive incidents, thus contributing to advancements in IoT-centric home security. By marrying RTS-DELM with blockchain, not only is the security of smart homes improved, but also the management and oversight of an extensive array of smart devices become more streamlined, leading to a more secure and efficient home environment.
Blockchain's role in smart home infrastructures also extends to addressing privacy by bolstering home automation systems against unauthorized access. While the architecture based on private blockchain ensures the privacy and security of data, it also invites considerations regarding scalability and performance, especially as the quantity of smart devices in homes increases. Moreover, the preservation of anonymity for users in these private networks is crucial. The study indicates a pressing need for blockchain technology to evolve, offering robust privacy and anonymity while maintaining or enhancing the scalability and performance of the network.

In summarizing the examination of these real-world applications, it becomes apparent that blockchain's integration with IoT represents a significant paradigm shift in technological implementation across diverse sectors. Each case study delineated herein not only exemplifies the versatility of blockchain technology but also its capability to revolutionize operational frameworks with enhanced security and efficiency. From the intricate web of global supply chains to the increasingly connected realm of smart home environments, blockchain emerges as a critical tool for ensuring data integrity, enhancing user agency, and bolstering systemic resilience. This exploration underscores the fact that blockchain's potential in conjunction with IoT extends far beyond its current applications, signaling a fertile ground for future research and development. The convergence of blockchain and IoT, as evidenced in these varied scenarios, paves the way for innovative solutions that promise to redefine industry standards and operational modalities. Consequently, this segment, while comprehensive, represents an initial foray into an expansive field replete with emerging opportunities and prospective advancements, setting the stage for further scholarly exploration and technological innovation in this dynamic domain.

B. VARIOUS PLATFORMS FOR BLOCKCHAIN

Implementing blockchain in the IoT infrastructure is definitely not an easy task.

The primary and essential step is to properly choose the blockchain-related platform that will be adopted to combine the IoT system with blockchain technology. There are several well-recognized platforms that can be used to implement blockchain in IoT. A comparison of these platforms is presented in Table 3.

TABLE III. Various platforms for blockchain

Platform	Type of blockchain	Smart contract	Consensus
Ethereum	Public and Permissioned	Yes	PoS
Hyperledger	Permissioned	Yes	PBFT
IOTA	-	Yes	-
Multichain	Permissioned	Yes	PBFT
Litecoin	Public	No	Scrypt
Lisk	Public and Permissioned	Yes	DPoS
HDAC	Permissioned	Yes	ePOW
Quorum	Permissioned	Yes	Multiple

Note. Adapted from "Emergent Converging Technologies and Biomedical Systems: Implementation of Blockchain in IoT" by Kaur, A. & Ali, A., 2022, p. 158. Copyright 2022 by Springer Science and Business Media LLC.

7. RESULTS AND DISCUSSION

This section critically evaluates the integration of blockchain technology with the Internet of Things (IoT), focusing on its role in addressing pivotal challenges such as system security, scalability enhancement, and privacy fortification. Through an extensive analysis of recent academic literature and practical case studies, we provide an integrated perspective on the transformative potential of blockchain in the IoT landscape.

Analysis of IoT Security and Privacy Issues: Analysis of IoT Security and Privacy Issues: Current research underscores the pressing demand for sophisticated security measures in IoT, as explored in "A Review of Security and Privacy Concerns in the Internet of Things (IoT) [33]." This study delineates a variety of security threats that IoT systems face, including malware and cyberattacks. Complementarily, "Blockchain Security and Privacy for the Internet of Things" [34] highlights how blockchain can fortify IoT security infrastructure. Our study affirms these findings, suggesting that blockchain stands as a crucial element in navigating through the intricate security issues present in IoT environments.

Role of Blockchain in IoT Infrastructure: Our review reveals blockchain's significant impact on IoT's infrastructural design, echoing the insights from "A Bibliometric Analysis of Blockchain Use for the RPL Technology: A Systematic Literature Review [35]" and "Blockchain–a promising solution to internet of things: A comprehensive analysis, opportunities, challenges and future research issues. [36]" These studies illustrate how blockchain aligns with the decentralized nature of IoT and offers scalable, efficient solutions, supporting our synthesis on the importance of blockchain in strengthening the infrastructure of IoT networks.

Blockchain in IoT Data Management: In examining blockchain's role in IoT data management, we find parallels in "Analysis of Blockchain Solutions for IoT: A Systematic Literature Review" and "Blockchain Technology for the Industrial Internet of Things". [1],[37] These references highlight the efficacy of blockchain in managing and securing large-scale IoT data, aligning with our literature analysis on blockchain's capabilities in enhancing data integrity and facilitating secure data exchange within IoT networks.

Enhancing IoT Device Management through Blockchain: Our literature review indicates that blockchain significantly improves IoT device management, a finding supported by "Embedding Blockchain Technology into IoT for Security: A Survey [38]" and "Resolving Security Issues in the IoT Using Blockchain [39]." These studies detail blockchain's ability to address administrative and security challenges in IoT networks, validating our analysis on blockchain's contribution to more efficient and secure management of IoT devices.

Implications of Blockchain in IoT: A Literature Perspective: Reflecting on the broader implications of blockchain in IoT, our review aligns with insights from "State-of-the-Art Research in Blockchain of Things for HealthCare" [40] and "The Blockchain Internet of Things Review, Opportunities, Challenges, and Recommendations." [41] These studies explore how blockchain can mitigate various security threats, echoing our synthesized view on blockchain's transformative potential in diverse industrial sectors, enhancing resilience and trust in IoT ecosystems.

Scalability Challenges in IoT-Blockchain Integration: In our analysis of scalability challenges for IoT-blockchain integration, the decentralized structure of blockchain, as discussed in "Blockchain Applicability for the Internet of Things: Performance and Scalability Challenges and Solutions," shows promise for managing large IoT networks. Yet, current blockchain platforms, including Ethereum and Hyperledger Fabric, face limitations in scalability, highlighting a disparity between theoretical capabilities and practical scalability in expansive IoT systems [42]. This gap underscores the necessity for further research to optimize blockchain scalability in the IoT domain.

Privacy Concerns in IoT-Blockchain Ecosystems: In addressing privacy concerns within IoT-blockchain ecosystems, it's crucial to distinguish between security and privacy. As highlighted in "The Internet of Things ecosystem:

The blockchain and privacy issues," while blockchain's security features are robust, they do not automatically equate to privacy compliance. The paper advocates a 'privacy by design' approach, where privacy considerations are integral to system development, focusing on protecting user data from the outset. This approach is particularly relevant under stringent legal frameworks like the GDPR. The immutable nature of blockchain, although secure, presents unique challenges in privacy management, necessitating a careful balance between technological solutions and legal obligations [43].

Concluding this analysis, it is evident that blockchain technology is not just a solution but a transformative force in the IoT realm. It promises to bring about a more robust, transparent, and efficient ecosystem, redefining the boundaries of IoT capabilities. This evolution highlights the imperative for continued research and practical implementation of blockchain in IoT, steering the course towards a future marked by enhanced security and trust in interconnected digital systems.

8. FUTURE RESEARCH DIRECTIONS

The integration of blockchain with IoT heralds promising advancements in security and scalability, but it also unveils a spectrum of challenges that need addressing to fully harness the capabilities of IoT applications. Drawing insights from the discussions in Section VII, this section outlines key areas that warrant further exploration and innovation.

Enhancing Scalability in Blockchain for IoT: A pivotal area for future research is the enhancement of blockchain's scalability to accommodate the high data throughput and transaction volumes characteristic of IoT applications. This necessitates the exploration of innovative blockchain architectures or hybrid models specifically tailored to manage the expansive network connectivity and data demands of large-scale IoT networks. Furthermore, the integration of advanced consensus mechanisms that can operate efficiently at scale and the optimization of blockchain nodes for IoT-specific functionalities are essential. Such advancements are crucial for ensuring that blockchain technology can effectively support the growth and complexity of IoT systems.

Addressing Privacy and Anonymity: As data privacy concerns continue to escalate, particularly in IoT applications, there is a pressing need for research focused on augmenting privacy and anonymity within blockchain infrastructures. This includes the development of advanced cryptographic methods and the adaptation of blockchain to comply with stringent data protection regulations, such as the GDPR. Moreover, incorporating zero-knowledge proofs to allow transaction verification without revealing underlying data, and enhancing the interoperability of privacy-preserving mechanisms across different blockchain platforms are vital steps. Emphasizing privacy by design and embedding these principles into blockchain systems from inception will be instrumental in safeguarding user data.

Resource Constraints and IoT Node Processing: Another critical research domain is overcoming the resource limitations of IoT nodes. Innovative solutions are required to enable IoT nodes to process and communicate transactions directly to the blockchain while mitigating their constrained processing capabilities. This could involve creating more lightweight blockchain protocols or designing efficient sensor gateways that alleviate the computational and memory demands on IoT devices. Additionally, employing edge computing to preprocess data locally before blockchain integration can reduce latency and enhance node performance. Developing adaptive algorithms that dynamically adjust resource allocation based on real-time node capabilities and network conditions will further optimize IoT operations.

Challenges of Big Data in Blockchain-IoT Systems: The amalgamation of Big Data Analytics (BDA) with blockchain in IoT infrastructures presents significant challenges, stemming from the anonymity of blockchain data and the resource limitations of IoT devices. Future investigations should focus on creating methodologies that facilitate effective data analysis within blockchain frameworks, and on developing BDA strategies that are compatible with the resource constraints of IoT nodes. Efforts should also include enhancing data preprocessing techniques to ensure efficient handling and analysis of vast amounts of data generated by IoT devices, and implementing scalable machine learning algorithms that can operate within the decentralized nature of blockchain networks..

Security Vulnerabilities: While blockchain inherently bolsters IoT system security, it is not devoid of vulnerabilities. Future research endeavors should delve into identifying and mitigating the security weaknesses inherent in blockchain systems, especially those related to smart contracts and potential interception risks, such as Border Gateway Protocol (BGP) vulnerabilities. Enhancing the security features of blockchain frameworks and reinforcing the defense mechanisms of IoT devices against these vulnerabilities are crucial steps towards a more secure IoT ecosystem. In addition, the development of more robust encryption techniques and the implementation of continuous security audits and updates can further safeguard blockchain and IoT integrations. Developing specific protocols for anomaly detection and real-time threat management will also play a vital role in enhancing system resilience.

The following Table 4 details several open research problems in the BC-IoT field, providing a concise overview of the key areas that require further investigation and development.

TABLE IV. Open research problems for BC-IoT

Research Direction	Description
Confidentiality breach	• A confidentiality breach can occur as a result of the entire transaction data being stored on the blockchain.
Security Vulnerability	• Blockchain systems have many security flaws, analogous to the shortcomings of smart contracts. • Some malicious users have the ability to use the Border Gateway Protocol (BGP) to intercept Decentralized messages.
Resource Constraints	• IoT nodes can be difficult to process when it comes to submitting transactions directly to the blockchain. • Blockchain-related Sensor gateways necessitate extensive processing capabilities and memory space to be a peer.
Scalability	• Several blockchain systems suffer from low data flow rate. • Blockchain systems may not be adequate for applications with a large volume of transactions, specifically for IoT.
Big Data challenge	• Given the resource constraints, IoT nodes are unable to use BDA approaches. • An information analysis on anonymous blockchain information is difficult to perform.

Note. Adapted from "A Survey on Blockchain for Industrial Internet of Things" by Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2022). Alexandria Engineering Journal, 61(8), 6001–6022. Copyright 2022 by Elsevier B.V.

9. CONCLUSION

This comprehensive review underscores that integrating blockchain technology within IoT frameworks emerges as a strategic solution to the profound security and privacy concerns inherent in IoT networks. The synergy of blockchain and IoT is poised to offer a plethora of benefits, including heightened trust, enhanced security and privacy, increased resilience and transparency, and more efficient data management. These benefits are expected to catalyze transformative changes across diverse sectors such as energy, supply chains, healthcare, retail, and transportation, highlighting the substantial impact of this integration.

However, the realization of this potential is contingent upon overcoming significant challenges, particularly in scalability, privacy, and anonymity. The scalability challenge is critical, given the rapidly growing number of IoT devices. This expansion necessitates blockchain solutions that can efficiently manage large volumes of data and sustain high transaction rates. Additionally, privacy and anonymity concerns are amplified by the inherent transparency of blockchain technology. Developing sophisticated solutions that uphold data protection while retaining the decentralized essence of blockchain is paramount.

The need to address these challenges is vital for unlocking the full potential of blockchain in IoT applications. Future research should thus focus on designing blockchain architectures that are not only scalable but also adept at bolstering privacy and anonymity. This endeavor will likely require innovative approaches that align blockchain's strengths with the unique demands of IoT systems.

The convergence of blockchain and IoT, while still in its nascent stages, holds immense potential and opens the door for extensive research and development. Tackling issues related to scalability, privacy, and anonymity is essential not just for overcoming current limitations, but also for laying the groundwork for novel and groundbreaking blockchain applications within the IoT landscape. These efforts are crucial for the future evolution of IoT, potentially leading to the emergence of new business models and significant shifts in various industries.

In conclusion, while the union of blockchain and IoT presents significant opportunities, it also poses substantial challenges that must be addressed through focused research and innovative problem-solving. The journey towards fully harnessing this powerful combination is ongoing, and its success will likely shape the future trajectory of technology, industry, and society.

References

[1] 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, p. 58822–58835, 2019. [Online]. Available: http://dx.doi.org/10.1109/access.2019.2914675

[2] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, p. 1250–1258, Oct. 2017. [Online]. Available: http://dx.doi.org/10.1109/jiot.2017.2694844

[3] R. H. Weber, "Internet of things: Privacy issues revisited," *Computer Law amp; Security Review*, vol. 31, no. 5, p. 618–627, Oct. 2015. [Online]. Available: http://dx.doi.org/10.1016/j.clsr.2015.07.002

[4] N. Aleisa and K. Renaud, "Privacy of the internet of things: A systematic literature review," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, ser. HICSS. Hawaii International Conference on System Sciences, 2017.

[5] A. Tewari and B. Gupta, "Security, privacy and trust of different layers in internet-of-things (iots) framework," *Future Generation Computer Systems*, vol. 108, p. 909–920, Jul. 2020. [Online]. Available: http://dx.doi.org/10.1016/j.future.2018.04.027

[6] T. Das and S. Mukherjee, *Data Privacy in IoT Network Using Blockchain Technology*. Springer Nature Singapore, 2022, p. 117–137. [Online]. Available: http://dx.doi.org/10.1007/978-981-19-0770-8_10

[7] L. K. Ramasamy and S. Kadry, *Industrial Internet of Things*. IOP Publishing, May 2021. [Online]. Available: http://dx.doi.org/10.1088/978-0-7503-3663-5ch2

[8] J. Mattila, T. Seppala, C. Naucler, R. Stahl, M. Tikkanen, A. Badenlid *et al.*, "Industrial blockchain platforms: An exercise in use case development in the energy industry," ETLA Working Papers, Working Paper, 2016.

[9] H. Hackbarth, "The three challenges of iot solution development," https://blog.bosch-si.com/internetofthings/the-three-challenges-of-iot-solution-development, accessed: [insert date here].

[10] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, p. 395–411, May 2018. [Online]. Available: http://dx.doi.org/10.1016/j.future.2017.11.022

[11] A. Hameed and A. Alomary, "Security issues in iot: A survey," in *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. IEEE, Sep. 2019.

[12] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, p. 8076–8094, Oct. 2019. [Online]. Available: http://dx.doi.org/10.1109/jiot.2019.2920987

[13] R. Anusha, M. Yousuff, B. Bhushan, J. Deepa, J. Vijayashree, and J. Jayashree, *Connecting Blockchain with IoT—A Review*. Springer Nature Singapore, 2022, p. 141–148. [Online]. Available: http://dx.doi.org/10.1007/978-981-16-8721-1_14

[14] A. Banafa, *Three Major Challenges Facing IoT*. River Publishers, May 2023, p. 29–36. [Online]. Available: http://dx.doi.org/10.1201/9781003426240-6

[15] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in iot using blockchain," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*. IEEE, Oct. 2017.

[16] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with iot to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, p. 54478–54497, 2021. [Online]. Available: http://dx.doi.org/10.1109/access.2021.3070555

[17] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in iot: challenges and solutions," *Blockchain: Research and Applications*, vol. 2, no. 2, p. 100006, Jun. 2021. [Online]. Available: http://dx.doi.org/10.1016/j.bcra.2021.100006

[18] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, p. 352, 2018. [Online]. Available: http://dx.doi.org/10.1504/ijwgs.2018.095647

[19] Les Notes Scientifiques de l'Office, "Comprendre les blockchains," Online, April 2018, https://www.senat.fr/rap/r17-584/r17-584-syn.pdf.

[20] R. Kumar, F. Khan, S. Kadry, and S. Rho, "A survey on blockchain for industrial internet of things," *Alexandria Engineering Journal*, vol. 61, no. 8, p. 6001–6022, Aug. 2022. [Online]. Available: http://dx.doi.org/10.1016/j.aej.2021.11.023

[21] I. B. Senkyire and Q.-A. Kester, "Validation of forensic crime scene images using watermarking and cryptographic blockchain," in *2019 International Conference on Computer, Data Science and Applications (ICDSA)*. IEEE, Jul. 2019.

[22] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys amp; Tutorials*, vol. 21, no. 2, p. 1676–1717, 2019. [Online]. Available: http://dx.doi.org/10.1109/comst.2018.2886932

[23] D. Vujicic, D. Jagodic, and S. Randic, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*. IEEE, Mar. 2018.

[24] A. Rayes and S. Salam, *The Blockchain in IoT*. Springer International Publishing, 2022, p. 277–303. [Online]. Available: http://dx.doi.org/10.1007/978-3-030-90158-5_10

[25] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A survey of iot and blockchain integration: Security perspective," *IEEE Access*, vol. 9, p. 156114–156150, 2021. [Online]. Available: http://dx.doi.org/10.1109/access.2021.3129697

[26] R. Kabir, A. S. M. T. Hasan, M. R. Islam, and Y. Watanobe, "A blockchain-based approach to secure cloud connected iot devices," in *2021 International Conference on Information*

and Communication Technology for Sustainable Development (ICICT4SD). IEEE, Feb. 2021.

[27] Y. V. R. S. Viswanadham and K. Jayavel, *Blockchain Implementation in IoT Privacy and Cyber Security Feasibility Study and Analysis*. Springer Singapore, 2022, p. 259–271. [Online]. Available: http://dx.doi.org/10.1007/978-981-16-9885-9_22

[28] V. Tsoukas, A. Gkogkidis, A. Kampa, G. Spathoulas, and A. Kakarountas, "Enhancing food supply chain security through the use of blockchain and tinyml," *Information*, vol. 13, no. 5, p. 213, Apr. 2022. [Online]. Available: http://dx.doi.org/10.3390/info13050213

[29] S. Ali, Abdullah, T. P. T. Armand, A. Athar, A. Hussain, M. Ali, M. Yaseen, M.-I. Joo, and H.-C. Kim, "Metaverse in healthcare integrated with explainable ai and blockchain: Enabling immersiveness, ensuring trust, and providing patient data security," *Sensors*, vol. 23, no. 2, p. 565, Jan. 2023. [Online]. Available: http://dx.doi.org/10.3390/s23020565

[30] A. Rejeb, K. Rejeb, S. Simske, H. Treiblmaier, and S. Zailani, "The big picture on the internet of things and the smart city: a review of what we know and what we need to know," *Internet of Things*, vol. 19, p. 100565, Aug. 2022. [Online]. Available: http://dx.doi.org/10.1016/j.iot.2022.100565

[31] G. Manogaran, M. Alazab, P. M. Shakeel, and C.-H. Hsu, "Blockchain assisted secure data sharing model for internet of things based smart industries," *IEEE Transactions on Reliability*, vol. 71, no. 1, p. 348–358, Mar. 2022. [Online]. Available: http://dx.doi.org/10.1109/tr.2020.3047833

[32] M. S. Farooq, S. Khan, A. Rehman, S. Abbas, M. A. Khan, and S. O. Hwang, "Blockchain-based smart home networks security empowered with fused machine learning," *Sensors*, vol. 22, no. 12, p. 4522, Jun. 2022. [Online]. Available: http://dx.doi.org/10.3390/s22124522

[33] M. Aqeel, F. Ali, M. W. Iqbal, T. A. Rana, M. Arif, and M. R. Auwul, "A review of security and privacy concerns in the internet of things (iot)," *Journal of Sensors*, vol. 2022, p. 1–20, Sep. 2022. [Online]. Available: http://dx.doi.org/10.1155/2022/5724168

[34] M. Picone, S. Cirani, and L. Veltri, "Blockchain security and privacy for the internet of things," *Sensors*, vol. 21, no. 3, p. 892, Jan. 2021. [Online]. Available: http://dx.doi.org/10.3390/s21030892

[35] J. Teddy Ibibo, "A bibliometric analysis of blockchain use for the rpl technology: A systematic literature review," *International Journal of Science and Research (IJSR)*, vol. 12, no. 9, p. 1219–1242, Sep. 2023. [Online]. Available: http://dx.doi.org/10.21275/sr23913192416

[36] A. K. Paul, X. Qu, and Z. Wen, "Blockchain–a promising solution to internet of things: A comprehensive analysis, opportunities, challenges and future research issues," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, p. 2926–2951, Apr. 2021. [Online]. Available: http://dx.doi.org/10.1007/s12083-021-01151-0

[37] S. Latif, Z. Idrees, Z. e Huma, and J. Ahmad, "Blockchain technology for the industrial internet of things: A comprehensive survey on security challenges, architectures, applications, and future research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, Jul. 2021. [Online]. Available: http://dx.doi.org/10.1002/ett.4337

[38] L. D. Xu, Y. Lu, and L. Li, "Embedding blockchain technology into iot for security: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 13, p. 10452–10473, Jul. 2021. [Online]. Available: http://dx.doi.org/10.1109/jiot.2021.3060508

[39] H. A. M. Malik, A. A. Shah, A. H. Muhammad, A. Kananah, and A. Aslam, "Resolving security issues in the iot using blockchain," *Electronics*, vol. 11, no. 23, p. 3950, Nov. 2022. [Online]. Available: http://dx.doi.org/10.3390/electronics11233950

[40] J. Almalki, "State-of-the-art research in blockchain of things for healthcare," *Arabian Journal for Science and Engineering*, May 2023. [Online]. Available: http://dx.doi.org/10.1007/s13369-023-07896-5

[41] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "The blockchain internet of things: review, opportunities, challenges, and recommendations," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, p. 1673, Sep. 2023. [Online]. Available: http://dx.doi.org/10.11591/ijeecs.v31.i3.pp1673-1683

[42] Z. Rahman, X. Yi, S. T. Mehedi, R. Islam, and A. Kelarev, "Blockchain applicability for the internet of things: Performance and scalability challenges and solutions," *Electronics*, vol. 11, no. 9, p. 1416, Apr. 2022. [Online]. Available: http://dx.doi.org/10.3390/electronics11091416

[43] N. Fabiano, "The internet of things ecosystem: The blockchain and privacy issues. the challenge for a global privacy standard," in *2017 International Conference on Internet of Things for the Global Community (IoTGC)*. IEEE, Jul. 2017.

Yassine MAADALLAH , a Master of Science graduate in Data Engineering and Software Development from Mohammed V University, Rabat, is currently pursuing doctoral studies at the Engineering Sciences Laboratory, ENSA de Kenitra, Ibn Tofail University. His research primarily focuses on the Internet of Things (IoT) and Blockchain technology. He can be reached for professional inquiries at yassine.maadallah@uit.ac.ma.

Nassira KASSIMI , a doctoral student at the Engineering Sciences Laboratory, ENSA de Kenitra, affiliated with Ibn Tofail University, specializes in IoT and Blockchain technology. She holds a Master's in Microelectronics, Telecommunications, and Industrial Information Systems from Sidi Mohamed Ben Abdellah University, Fes. Alongside her research, she teaches at the Saudi School in Rabat. Contact her for collaborations at kassimi.nassira@gmail.com.

Younès EL BOUZEKRI EL IDRISSI , a professor at ENSA, Ibn Tofail University, Kenitra, and a member of the Engineering Sciences Laboratory, holds a Doctorate in Computer Science from ENSIAS. Specializing in various computer science areas, Younès EL BOUZEKRI EL IDRISSI actively contributes to both academia and industry. For inquiries or collaborations, contact Younès EL BOUZEKRI EL IDRISSI at y.elbouzekri@gmail.com.

Youssef BADDI , a professor at Higher School of Technology, Chouaib Doukali University, is a notable figure in computer science, holding a doctorate from the National School of Computer Science and Systems Analysis, University Mohamed V, Rabat. Renowned for his work at the STIC Laboratory, his expertise is well-respected academically and scientifically. Contact him for inquiries or collaborations at baddi.y@ucd.ac.ma.