International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

A survey of Blockchain integration with IoT: benefits, challenges and future directions

Yassine MAADALLAH[1], Nassira KASSIMI[1], Younès EL BOUZEKRI EL IDRISSI[1], 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

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

Received ## Mon. 20##, Revised ## Mon. 20##, Accepted ## Mon. 20##, Published ## Mon. 20##

Abstract: The Internet of Things (IoT) has emerged with the emergence of the new generation of information technologies as a central and recognized concept that enables large-scale capabilities, and it also enables seamless integration and collaboration between virtual and real entities, paving the way for a large number of transformative digital services aimed at improving the user experience.

Despite the many advantages and benefits of the Internet of Things, it poses challenges that require in-depth study, particularly in the areas of security, simplicity and data integration. The aim of this paper is to examine these challenges in depth, explore potential strategies for addressing them, mitigate risks and ensure a safe and reliable environment for the Internet of Things.

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

I. INTRODUCTION

As IoT technologies evolve and are used extensively, security issues and a sense of vulnerability have arisen among IoT users. Such constraints hinder the exploration and improvement of data privacy and security in the IoT, and moving to a decentralized ledger technology might be the right solution to address these issues.

Blockchain technology is the most popular of these innovation and integrate blockchain with the Internet of Things (IoT) can produce incalculable benefits, because IoT leverages because IoT leverages blockchain technology to save transactions, to increase performance, to deliver additional security and to provide platforms that are distributed. The purpose is to gain a good comprehension of the security and confidentiality functionalities of blockchains and the possibilities of implementation in diverse domains integrated with the IoT. This article will enable new researchers to develop future Blockchain-IoT systems.

This study is organized as follows. Section two sheds light on the definition of Internet of Things (IoT) technology, as well as a presentation of security and the role of blockchain within the IoT. Section three explains the key principles and functionality of blockchain, along with a brief description of the technology's operating mechanism. Section four outlines the security and backup benefits of blockchain for the IoT. Section five looks at the different blockchain platforms. In section six, we integrate the most recent considerations as well as avenues for future research. Finally, section seven concludes the paper.

II. AN OVERVIEW OF IOT: EXPLORING ITS ARCHITECTURE AND CHALLENGES

1. DEFINITION OF IOT

Today IoT is among the most important technologies of the 21st century, it is an interconnected network that 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 with other objects on the internet. It is invented by Smart devices with web connectivity that are capable of organizing, transmitting and reacting to any data from their respective embedded systems [1].

The IoT framework enables intelligent sensing of various information extracted from diverse applications before it is securely transmitted to the server [1].

The domain of " IoT " (Internet of Things) greatly expanded in the last several years because of the quantity of objects that have been augmented and the quality of gadgets that have been improved, which will lead to financial profitability as well as other social benefits that simplify the daily lives of individuals using this new technology [1].

2. IoT Architecture

The structure of IoT mainly consists of three layers, Table 1 below represents these three layers:

Table 1
IoT Composite Layers

Layers	Description
IoT sensing layer	Also called Perception layer is the first in the IoT architecture and is in charge of collecting data via various devices. such as sensors, actuators and Internet-connected gateways that interact with each other to achieve this goal. This data extracted from the physical world is sent to the next phase of the IoT architecture for 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: This table was 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. (pp. 147). Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-16-8721-1_14.

Recently, another layer has been introduced, called "Support" or "Middleware" layer. This layer is situated in the middle of the connectivity and the software layer. As shown in figure 1 below, it has advanced features such as storage, computation, processing and action taking capabilities.

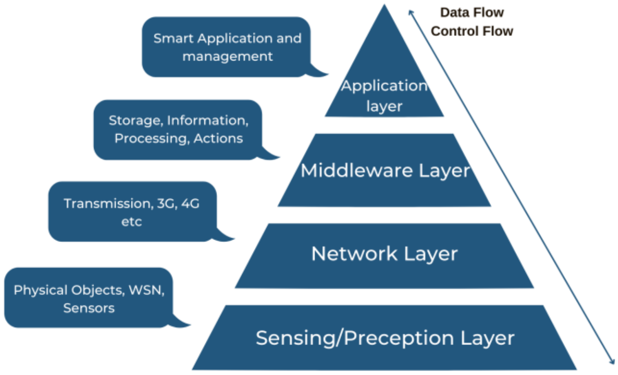

Fig 1: Multi-layered architectural view of IoT

3. Blockchain roles to address IoT challenges.

One of the most significant aspects of the IoT is its ability to deploy rapidly in diverse sectors such as industry, agriculture, people's daily lives, healthcare, IT, data analytics, and many others. What's more, the IoT integrates easily with other technologies such as “Blockchain, Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), etc” [3].

A. The challenges of IoT

The IoT solves many problems in different sectors, making it one of the biggest opportunities and solutions for businesses and industries worldwide. However, despite the benefits it offers, IoT systems also face various challenges.

- Scalability: Today the world is connected via smart gadgets such as phones and TVs which are all connected in a massive network, which will make managing the data sent a bit difficult hence the use of massive data analysis and cloud storage is essential [4].
- Heterogeneity and diversity: Product vendors aspire to introduce new services like predictive maintenance and usage billing by leveraging device connectivity and cloud-based applications. Despite all this, the biggest challenge of the Internet of Things remains the problem that product vendors face in terms of controlling the heterogeneity of their device portfolio in the Internet of Things [5].
- Privacy, confidentiality and data integrity: Due of the massive user base for IoT, their data goes over many hops in the network system, so it is necessary to encode this data to keep it confidential to prevent all unauthorized users from access to user's data [6].

- Security: The system must ensure the security of all users who share the network and attempt to access other data. IoT security risks are different for each layer, while security is incredibly important to an enterprise [7].
- Given the extreme difficulty of implementing security countermeasures in resource-constrained IoT systems, "traditional solutions such as authentication, authorization, and communication encryption are not adapted to the IoT" [8]. In addition, the lack of timely security firmware updates makes the Internet of Things vulnerable to many malicious attacks¬.
- Immutability: data changes in the network result in a loss of security that can lead to privacy issues in the participating nodes. Such immutability has been extremely challenging in the IoT [9].

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 [10].
- 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 [10].
- 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 [10].
- 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 [11].
- Common IoT applications include connecting surveillance robots, wearable biometric systems for combat, aircraft, tanks, soldiers and even drones via an interconnected system.

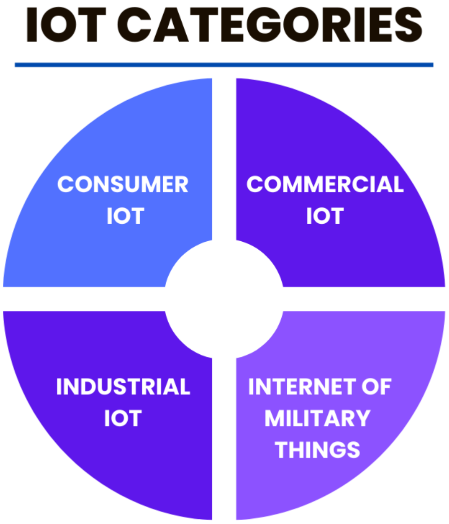

Fig 2: Types of IoT Devices

C. *The role of blockchain in the IoT technology*

Today's IoT systems are composed of a very large number of devices, objects and many sensors that are interconnected to perform many various operations in an IoT environment. Processing and controlling the huge amount of existing devices is very complicated, and the current security model of centralized servers used to store, authenticate and analyze data, exposes the risk of network attacks during this process is very high [12].

A essential solution to the privacy and security issues faced by IoT can be found in Blockchain technology, using intelligent contracts, which are extremely important in the process of managing and securing devices of the IoT [12].

The advantages of combining the technology of blockchain and IoT are numerous, as shown in the figure below:

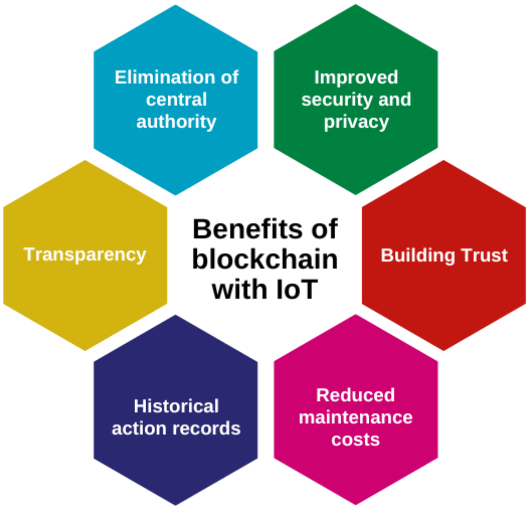
Elimination of central authority
Improved security and privacy
Transparency
Benefits of blockchain with IoT
Building Trust
Historical action records
Reduced maintenance costs

Fig 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 [12].

- Improved security and privacy: Network security is among the most important challenges facing the IoT. The blockchain is therefore the ideal solution to guarantee the confidentiality and security of data by saving them in the form of encrypted transactions digitally signed by encryption keys. In addition, the use of intelligent contracts may provide better solutions to enhance the safety of IoT systems by auto upgrading the firmware of IoT devices [8].

- 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 [12].

- 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 [8].

- Transparency: Typically, IoT users do not have the ability to know where and how the data they provide is being used, and the lack of transparency is one of the biggest challenges facing IoT technology, so blockchain can be used to solve the problem of lack of transparency. This is because the data stored in blockchains is more accurate and transparent than that found on traditional networks. This transparency helps protect the believability of blockchain-based systems by restricting the opportunity for unauthorized data modification. Since it is impossible to change a transaction in the blockchain without using consensus, this means that all participants in the network must agree, as all users of the blockchain have the same rights on the network to bind, verify, and track transactional activities [13].

- Reduced Cost: Cost reduction is one of the main objectives of many companies. This step is very important as it consists in 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.

III. Overview of the Blockchain

1. Definition of Blockchain

The blockchain can be considered as a collaborative registry that stores the data generated in a network by several users. Technically, it is a distributed database in which the data sent by users is stored as a public ledger on a permanent basis in a decentralized environment[14].

The blockchain is composed of several blocks linked together by a chain, with each block contains a timestamp and a transaction message protected by public key cryptography. The encryption concept used by the blockchain, combined with a Secure digital signature and a distributed consensus algorithm, makes it decentralized and reliable [15].

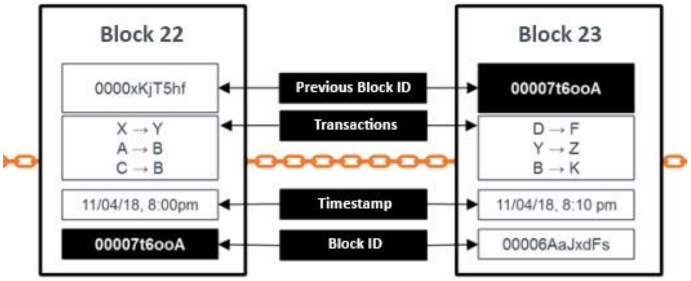

Fig 4: Block structure

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 [16]. 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).

2. BLOCKCHAIN COMPONENTS

Blockchain consists of several concepts such as transaction, block. In this section, we present these different components.

A. *The block*

A blockchain is created by connecting a group of blocks that store a set of data.. This explains why the block is the basic element for the proper functioning of a blockchain. Every block can be viewed as a sheet of the ledger. A block is a record in the blockchain, which contains and confirms several pending data or transactions.

It is essentially comprised of the attributes and details of the block.

a) Block header:

Specifically, the block header includes[1]:

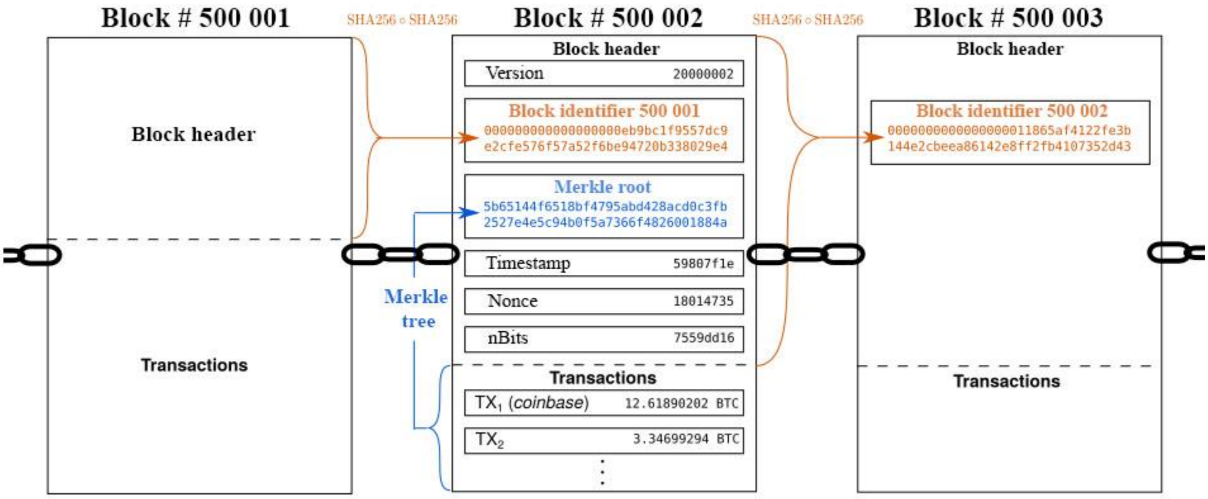

Fig 5: Block structure

- 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 [3].

B. 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.

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:

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.

C. Transactions and digital signatures

Peers on the blockchain network rely on a public-private key pair to perform transactions, whether they are crypto-currency or a simple data exchange. These private keys are used by peers to be able to make signed transactions and use the address of the peer on the recipient's blockchain to pass the transaction to them. These addresses are generated by computing the cryptographic hash of the user's public key [17].

For example, SHA-256 encryption is performed in the case of bitcoin to extract user addresses, which has the effect of masking the transparency of the public keys of blockchain peers in crypto-currency applications. Since there are no sequential tokens, a number of tokens are initially associated with addresses present in the initial parts of the blockchain. Transactions keep track of token ownership by increasing or decreasing the tokens associated with each address participating in executions outside the crypto-currency. Transactions do not define token ownership, they are based solely on the sharing of data protected by digital signatures[17].

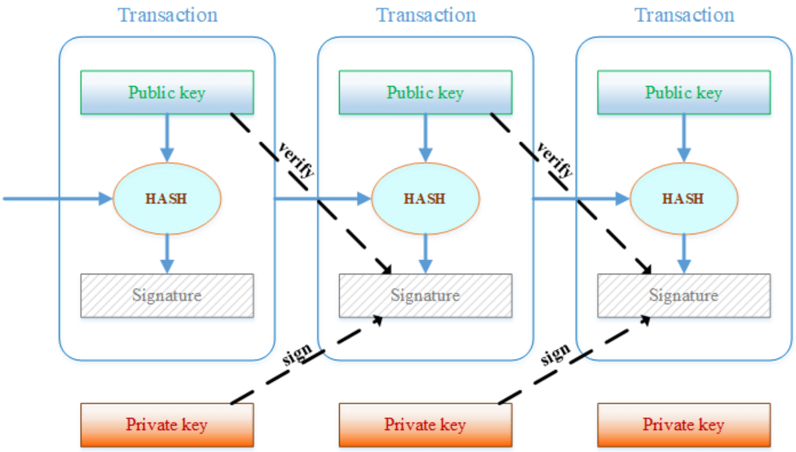

Fig 6: The structure of transaction in a Bitcoin blockchain

We take the case of Alice for example to understand how blockchain transactions function and execute in unencrypted execution processes, where Alice encrypts the transaction information before sending part of it to Bob using her public key. She then takes a hash of the sent data and encrypts it with her private key to create a cryptographic signature. Each transaction consists of the encrypted data itself and the digital signature embedded in the transaction header. The transaction is then published on the distributed ledger network. As the transaction is addressed to Bob, he must decrypt the digital signature using Alice's public key to verify the contents of the transaction, and then decrypt its data using his private key. This process is characterized by simplicity and clarity because of the comparison between the data hash and the digital signature[17].

D. 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[15].

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[15].

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

a) Proof-of-Work (PoW)

This is the best known mechanism at the moment. It is the most famous blockchain consensus algorithm applied in bitcoin.

The fundamental aspect of the Proof of Work (PoW) protocol is that each node in the blockchain can participate in the creation of new blocks by proving that it has done computationally expensive work. Adding new blocks under the PoW algorithm is called "mining". Miners are the nodes of the network that are rewarded for their calculations with bitcoins and sometimes a commission on certain transactions[15].

In terms of network security, miners add most of the blocks in the longest chain because of its reliability. Therefore, the PoW mechanism is secure as long as 51% of the hashing power is held by legitimate network participants [15].

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[1]. 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 [9].

The advantage of using PoS in the place of PoW is the cost effectiveness because it uses much less energy so Pos

yassine.maadallah@uit.ac.ma, kassimi.nassira@gmail.com, y.elbouzekri@gmail.com, baddi.y@ucd.ac.ma

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[15].

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[17].

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[17].

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)

Intel has recently developed a new blockchain consensus algorithm, it is a bit different from the consensus algorithms we talked about earlier. It was designed for the Hyperledger Sawtooth Blockchain project [18].

Before a new block is created, each node is provided with a random trust time and the next block will be mined by the validator with the shortest wait time. the PoET consensus algorithm is based on trusted platform Software Guard Extensions (SGX) [13].

The PoET approach has the advantage of being much more power efficient compared to other consensus algorithms such as PoS and PoW. It does not need expensive hardware or high-end computational capacity. From all this, we conclude that Proof of Elapsed Time is a powerful solution for private IoT blockchain.

E. Smart contract

A blockchain is created by connecting a group of blocks that store a set of data.. This explains why the block is the basic element for the proper functioning of a blockchain. Every block can be viewed as a sheet of the ledger. A block is a record in the blockchain, which contains and confirms several pending data or transactions.

Introduced in the 1990s, they are programmable applications for enabling monetary transactions and storing important data in the blockchain under specific conditions[8]. The smart contract is executed as soon as the specified condition is triggered, without the assistance of any intermediary, It is intended to replace traditional contracts as an effective and safe solution.

Smart contracts allow IoT devices to automate preagreed actions, providing a new set of functionality for IoT solutions[15].

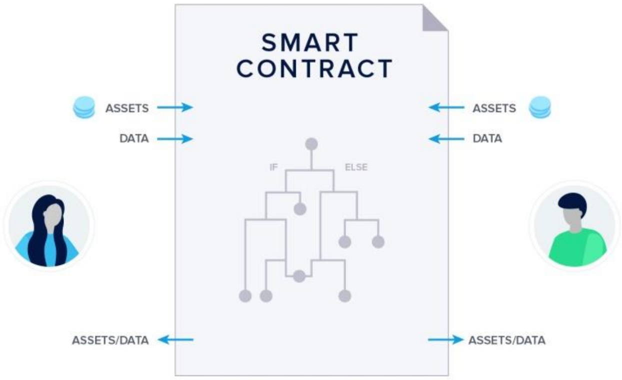

Fig 7: Diagram showing how a smart contract works

IV. TAXONOMIES AND KEY CHARACTERISTICS OF BLOCKCHAIN

1. 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: A blockchain is a sequence of interconnected blocks, whose each one is in fact an inverse hash point of the previous block. In parallel, the hash of the root of the Merkle tree saves the hash of all the transactions that participate in it. Any change to a transaction results in the creation of a new Merkle root. Consequently, any possible fraud can be immediately detected. The combination of the various hash points and the Merkle tree can guarantee the veracity of the information [3].

- 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 [3].

- 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 [12].

- 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 [3].

- Non-repudiation: In the blockchain, we use the private key to append a signature to the transaction, which can be viewed and verified by other users using the corresponding public key. A cryptographically signed transaction cannot therefore be rejected by the original initiator of the transaction [8].

- 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 [12].

- 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 [3].

2. 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[119].

- Private blockchain: Appropriate for companies operating in a restricted environment under a structured administration where only certain members can join the blockchain network. [19].

- 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[3].

Table 2 presents a comparison of blockchain types.

Table 2

Comparative analysis of the different types of blockchain and their key characteristics

Key Characteristics	Public Blockchain	Private Blockchain	Consortium Blockchain
Scalability	Limited Capabilities	Highly Scalable	Noteworthy Scalability
Decentralization	Entirely Decentralized	Centralized	Semi-Decentralized
Flexibility	Restricted Flexibility	High Malleability	Moderate Flexibility
Consensus	PoW, PoS Techniques	Employs Ripple	Utilizes PBFT, PoA, PoET
Transparency	Completely Visible	Hidden	Semi-Visible
Traceability	Fully Traceable	Fully Traceable	Semi-Trackable
Immutability	Unalterable	Subject to Changes	Semi-Unalterable

Note. This table was adapted from "A Survey on Blockchain for Industrial Internet of Things," by R. L. Kumar, F. Khan, S. Kadry, & S. Rho, 2022, Alexandria Engineering Journal, 61(8), p. 6009. https://doi.org/10.1016/j.aej.2021.11.020

V. Integration and Deployment of Blockchain with IoT

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 3
Comprehensive review of blockchain implementations

Blockchain Solution	Type of Implementation	Smart Contract Provision	Consensus Mechanism
Ethereum	Accessible to Public and Granted Permissions	Supported	PoS
Hyperledger	Access Granted via Permissions	Supported	PBTF
IOTA	-	Supported	-
Multichain	Access Granted via Permissions	Supported	PBTF
Litecoin	Accessible to Public	Not Supported	Scrypt
Lisk	Accessible to Public and Granted Permissions	Supported	DPoS
HDAC	Access Granted via Permissions	Supported	ePOW
Quorum	Access Granted via Permissions	Supported	Multiple Protocols

Note: This table was adapted from "Emergent Converging Technologies and Biomedical Systems: Implementation of Blockchain in IoT," by A. Kaur & A. Ali, Springer Science and Business Media LLC, p. 158. https://doi.org/10.1007/978-981-16-8774-7_13

VI. Future Research Directions

The fusion of blockchain and IoT presents many opportunities to improve security and scalability, increasing the ability of blockchain to accommodate future high-volume, large-scale IoT applications. However, many challenges must be addressed before IoT applications can be fully utilized. Table 5 provides an overview of open research problems about the integration of blockchain and the IoT.

Table 5
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) network routing protocol 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: This table was adapted from "A Survey on Blockchain for Industrial Internet of Things" by Kumar, R. L., Khan, F., Kadry, S., & Rho, S., 2022, p. 6014. Alexandria Engineering Journal, 61(8), 6001–6022. https://doi.org/10.1016/j.aej.2021.11.020.

VII. CONCLUSION

In conclusion, this review paper has explored the integration of blockchain technology in IoT applications as a potential solution to address the security and privacy challenges faced by IoT systems. The combination of blockchain and IoT offers numerous benefits such as trust, security, privacy, resiliency, transparency, and efficient data management. Moreover, blockchain's features of decentralization, security, and trust can enhance the functionality of IoT systems in various fields, including M2M communication, energy management, supply chain management, healthcare, retail, and transportation.

However, it is important to consider the challenges that still exist in the implementation of blockchain technology in IoT, such as scalability, privacy, and anonymity. Further research is required to address these challenges and fully realize the potential of blockchain in the IoT domain. Despite these challenges, it is clear that the integration of blockchain technology in IoT has the potential to revolutionize machine-to-machine communication and bring significant changes to various industries, leading to the development of new business models.

REFERENCES

[1] Das, T., & Mukherjee, S. (2022). Data Privacy in IoT Network Using Blockchain Technology. Intelligent Systems for Social Good, 117–137. https://doi.org/10.1007/978-981-19-0770-8_10

[2] Maadallah, Y. (2023). IoT Composite Layers [Table adaptation based on the book Micro-Electronics and Telecommunication Engineering, Connecting Blockchain with IoT—A Review by Anusha, R., Yousuff, M., Bhushan, B., Deepa, J., Vijayashree, J., & Jayashree, J., pp. 147]. Singapore: Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-16-8721-1_14

[3] Ramasamy, L. K., & Kadry, S. (2021). Industrial Internet of Things. Blockchain in the Industrial Internet of Things. https://doi.org/10.1088/978-0-7503-3663-5ch2

[4] Mattila, J., Seppala, T., Naucler, C., Stahl, R., Tikkanen, M., Badenlid, A., & al. (2016). Industrial Blockchain Platforms: An Exercise in Use Case Development in the Energy Industry. ETLA Working Papers

[5] Hackbarth, H. The three challenges of IoT solution development. https://blog.bosch-si.com/internetofthings/the-three-challenges-of-iot-solution-development

[6] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022.

[7] Hameed, A., & Alomary, A. (2019). Security Issues in IoT: A Survey. 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). https://doi.org/10.1109/3ict.2019.8910320

[8] Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A Survey. IEEE Internet of Things Journal, 6(5), 8076–8094. https://doi.org/10.1109/jiot.2019.2920987

[9] Anusha, R., Yousuff, M., Bhushan, B., Deepa, J., Vijayashree, J., & Jayashree, J. (2022). Connecting Blockchain with IoT—A Review. Lecture Notes in Networks and Systems, 141–148. https://doi.org/10.1007/978-981-16-8721-1_14

[10] Banafa, A. (2018). 6 Three Major Challenges Facing IoT. Secure and Smart Internet of Things (IoT): Using Blockchain and AI , River Publishers, 2018, pp.33-44

[11] Brown, T. (2020). What are IoT devices. https://itchronicles.com/iot/what-are-iot-devices

[12] Sadawi, A. A., Hassan, M. S., & Ndiaye, M. (2021). A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges. IEEE Access, 9, 54478–54497. https://doi.org/10.1109/access.2021.3070555

[13] Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in IoT: challenges and solutions. Blockchain: Research and Applications, 2(2), 100006. https://doi.org/10.1016/j.bcra.2021.100006

[14] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 14(4), 352. https://doi.org/10.1504/ijwgs.2018.095647

[15] Rayes, A., & Salam, S. (2022). The Blockchain in IoT. Internet of Things from Hype to Reality, 277–303. https://doi.org/10.1007/978-3-030-90158-5_10

[16] Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2022). A Survey on blockchain for industrial Internet of Things. Alexandria Engineering Journal, 61(8), 6001–6022. https://doi.org/10.1016/j.aej.2021.11.02

[17] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys &amp; Tutorials, 21(2), 1676–1717. https://doi.org/10.1109/comst.2018.2886932

[18] Shammar, E. A., Zahary, A. T., & Al-Shargabi, A. A. (2021). A Survey of IoT and Blockchain Integration: Security Perspective. IEEE Access, 9, 156114–156150. https://doi.org/10.1109/access.2021.3129697

[19] Viswanadham, Y. V. R. S., & Jayavel, K. (2022). Blockchain Implementation in IoT Privacy and Cyber Security Feasibility Study and Analysis. High Performance Computing and Networking, 259–271. https://doi.org/10.1007/978-981-16-9885-9_22

[20] Maadallah, Y. (2023). Comparison of blockchain types [Table adaptation based on the article "A Survey on Blockchain for Industrial Internet of Things" by Kumar, R. L., Khan, F., Kadry, S., & Rho, S., 2022, p. 6009]. Alexandria Engineering Journal, 61(8), 6001–6022. https://doi.org/10.1016/j.aej.2021.11.020

[21] Maadallah, Y. (2023). Various platforms for blockchain [Table adaptation based on the book "Emergent Converging Technologies and Biomedical Systems: Implementation of Blockchain in IoT" by Kaur, A. & Ali, A., pp. 158]. Springer Science and Business Media LLC. https://doi.org/10.1007/978-981-16-8774-7_13

[22] Maadallah, Y. (2023). Open research problems for BC-IoT [Table adaptation based on the article "A Survey on Blockchain for Industrial Internet of Things" by Kumar, R. L., Khan, F., Kadry, S., & Rho, S., 2022, p. 6014]. Alexandria Engineering Journal, 61(8), 6001–6022. https://doi.org/10.1016/j.aej.2021.11.020

Yassine MAADALLAH holds a Master's degree in Data Engineering and Software Development from the Faculty of Science at Mohammed V University in Rabat. He is currently pursuing a Ph.D. at the Engineering Sciences Laboratory in ENSA de Kenitra, affiliated with Ibn Tofail University in Kenitra. Yassine's research focuses on the exciting fields of IoT and Blockchain. For further communication, you can reach yassine.maadallah@uit.ac.ma

Nassira KASSIMI is a talented professional currently pursuing a Ph.D. at the Engineering Sciences Laboratory in ENSA de Kenitra, affiliated with Ibn Tofail University in Kenitra. She holds a Master's degree in Microelectronics, Telecommunications, and Industrial Information Systems from Sidi Mohamed Ben Abdellah University in Fes. With a research focus on IoT and Blockchain, Salma's expertise lies in exploring their applications and advancements. Alongside her academic pursuits, she serves as a permanent teacher at the Saudi School in Rabat. For further inquiries or collaborations, kindly reach out to Salma at kassimi.nassira@gmail.com

Younès EL BOUZEKRI EL IDRISSI is a professor at ENSA, affiliated to Ibn Tofail University in Kenitra. He is also a member of the Engineering Sciences Laboratory. Holder of a PhD in computer science from ENSIAS, Younès EL BOUZEKRI EL IDRISSI's expertise encompasses a wide range of subjects in the field. For further information, you can reach *y.elbouzekri@gmail.com*

Youssef BADDI a Ph.D. in Computer Science from the National School of Computer Science and Systems Analysis, University Mohamed V in Rabat. He is a distinguished Professor at the Higher School of Technology, Chouaib Doukali University. Additionally, Pr. Baddi serves as the Director of the STIC Laboratory. For further inquiries, you can reach Pr. Baddi at baddi.y@ucd.ac.ma