Sensors & Transducers, Vol. 256, Issue 2, March 2022, pp. 27-35

www.sensorsportal.com

Sensors & Transducers

Published by IFSA Publishing, S. L., 2022
http://www.sensorsportal.com

Opportunities and Challenges of IoT Security Using Distributed Ledger Technology

Chérif DIALLO
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept. Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

Received: 21 February 2022 /Accepted: 22 March 2022 /Published: 31 March 2022

Abstract: The Internet of Things (IoT) has finally made its way into people's daily lives. Multiple connected objects are present in many markets. Their rapid adoption is due to the fact that IoT applications are developing rapidly and are easily deployed. However, these applications present several security challenges, although they are based on existing network technologies, which are already more or less secure. These challenges can be broadly classified as identification, authentication, jamming, cloning, privacy, etc. To face these challenges and in the perspective of ensuring end-to-end IoT networks security, several encryption mechanisms have been adapted and widely used including public key infrastructure (PKI), AES standard and ECC (Elliptic Curve Cryptography). To correct the weaknesses and vulnerabilities that are still present, other technologies such as DLTs (Distributed Ledger Technology) have been recently adopted by the Internet of Things. This adoption is still in its infancy as there are no standards nor methods yet indicating how to manage the security of the IoT through DLTs. In this article, we review the IoT-DLT paradigm in order to identify the benefits and major challenges of the convergence of these two technologies.

Keywords: IoT, DLT, Blockchain, Security, Cloud.

1. Introduction

IoT (Internet of Things) systems have developed rapidly. Many people interact with the IoT on a daily basis without even realizing it. It may be present in a water supply system, in an electricity network, in transport or in healthcare providing system. IoT systems are connected to the internet, which presents a high risk of threats. If it is not sufficiently protected, the IoT could be could be the door open to many attacks with adverse effects. However, IoT security is a real challenge considering the limitations that characterize connected objects.

The use of cloud computing has proven to be advantageous because it allows secure storage, availability, accessibility and interoperability for IoT applications. However, in IoT-Cloud architecture, the cloud is a point of failure, and therefore availability and accessibility issues appear in case of an attack. This is why other solutions, such as DLTs, would be explored and seem promising. DLTs eliminate the trusted third party from the IoT-Cloud model. DLT based IoT architecture could provide solutions to accessibility and availability issues. Nevertheless, many challenges and questions remain to be explored for a good convergence of these two technologies. In

this paper, we present some key points on the DLT-IoT paradigm, and in particular on the use of DLT to secure the IoT environment.

The rest of the paper is organized as follows: in Section 2, we discuss IoT security issues. In Section 3, we present the fundamentals of DLTs, and then review recent works on IoT security using DLTs in Section 4. Finally, in Section 5, we describe the problems, challenges and future research directions before concluding in Section 6.

2. IoT Security Issues

The fairly widespread use of the Internet of Things make life easier. For example, the electricity supply chain, the water supply system, the smart farming and smart home applications are good illustrations. However, such IoT systems present hacking risks that could have harmful consequences [1, 2].

An IoT based water supply system in a city could be a vector for a terrorist attack consisting of corrupting connected objects in order to insert bacteria, viruses, or even worse, poisons without being detected. The consequences of such an attack could be very harmful for the whole population using this supply system.

A smart home has many connected devices such as fridges, TVs, locks, cameras, etc. As connected locks are designed to communicate with smartphones, the use of a specialized digital lock-picking application could allow hackers to make a physical intrusion into the premises.

Criminals could think of attacking a business through a connected electricity meter installed within this business in order to black out it. In another way, they could carry out larger attacks such as forcing a power plant to shut down through its computer system to cause a complete blackout.

Some attacks exploit connected devices as a means of accessing larger networks such as the Internet. The addition of a connected object to a secure infrastructure can create a new attack surface. The connected object can be used as a relay for a large scale attack.

Attacks [1, 2] such as Man-in-the-middle (MITM), DoS/DDoS, Sybil attack, which are very common in the internet network, are also inherited by IoT systems, (Fig. 1). So, IoT attacks are often intended to data or hardware theft, espionage, service compromise, system destabilization, etc. All these attacks could be carried out at different levels of the Internet of Things architecture (Fig. 1).

Therefore, securing an IoT System would mean securing the different levels of its architecture, which is not a trivial matter. Researchers are therefore working to provide security services such as authentication, availability, integrity, confidentiality, non-repudiation, scalability, transparency, reliable data storage, etc.

The encryption algorithms used for a long time and the security mechanisms used to ensure authentication and security of communication on the Internet have proved to be very energy consuming for IoT connected objects, which do not have much energy reserve.

.

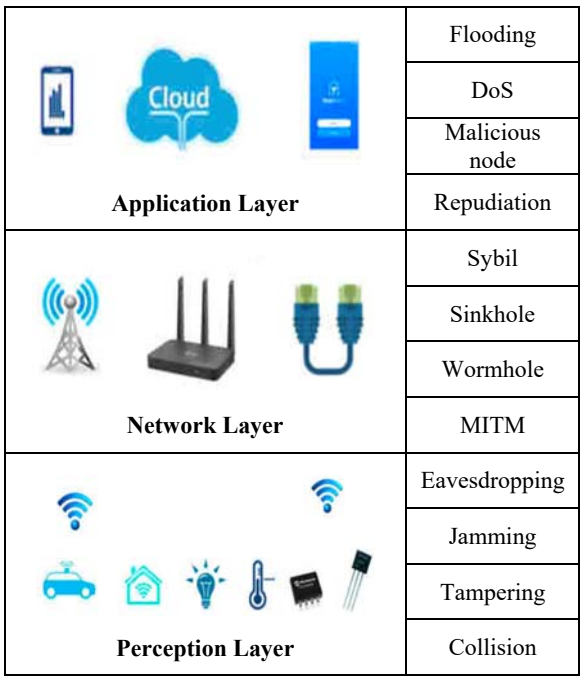

Fig. 1. IoT attacks.

On the other hand, IoT connected objects memory storage and computing power requirements do not facilitate the adoption of such algorithms. Thereby, a readjustment of these mechanisms is absolutely necessary. Similarly, the exploration of other efficient technologies in convergence with the IoT system has also its advantages.

Thus, cloud technology has been used to propel the IoT. The cloud has greatly contributed to the adoption of the Internet of Things in various domains (Table 1). It has 3 models:

- **Public cloud:** In the public cloud, resources are offered as a service, usually over an Internet connection, for a fee. Users can tailor their use on demand and do not need to buy hardware to use the service. In the public cloud, computing resources are open to a shared use [3].
- **Private cloud:** The aim is not to offer cloud services to the general public, but to use it within the organization. A private cloud is hosted in a company's data center and provides its services only to users within that company or its partners. A private cloud offers more security than the public cloud, and cost savings in case it would otherwise use unused capacity in an existing data center [3]. It is a model where all resources are reserved for the exclusive use of a company.
- **Hybrid cloud:** this is a mixture of public and private clouds. Hybrid clouds are more complex than the other deployment models, since they involve a composition of two or more clouds

(private or public). Each member remains a unique entity, but is bound to others through standardized or proprietary technology that enables application and data portability among them [3].

The cloud offers storage space, low-cost processing capacity (the customer only pays for what he uses), high availability, data accessibility and interoperability between IoT solutions [4]. However, the client-server model of the IoT-Cloud paradigm has many short comings. The cloud is a point of failure in the IoT-Cloud system.

A poorly configured public cloud (configuration flaws) could expose the data it stores on the internet. In a private cloud, an API to which objects will connect to send data and receive instructions, if it has a vulnerability, could be attacked in order to bounce into the company's network. This intrusion could then be used to steal industrial secrets. And if the API has an SQL injection vulnerability, the attacker will be able to use it to access the database to which the API is connected and thus gain access to private data. An attack on the cloud could have a direct impact on the IoT system.

The cloud has enabled the IoT to be easily usable in many cases, bringing many benefits. Apart from its security vulnerabilities, the cloud is opaque because participants do not know how their data is used.

Table. 1. IoT-Cloud paradigm benefits and deficiencies

IoT-Cloud paradigm	
Benefits	**Deficiencies**
Accessibility	Security
Connectivity	
Interoperability	Aupacity
Data analysis	
Real-time data translation	Trusted third party
Cost effective delivery	

To address the security deficit, other technologies such as DLTs are being explored. The combination of innovative technologies such as cloud computing and IoT has proven invaluable. DLTs are expected to further revolutionize the IoT by providing more security and establishing a reliable information sharing service that ensures that data is immutable [5, 6].

3. Fundamentals of Distributed Ledger Technologies (DLTs)

Distributed ledger technology is the generic term to describe any system that distributes data across multiple sites. A distributed registry is a decentralized database distributed across multiple computers or nodes. Each node will maintain the registry and if data changes, the registry will be updated. Each update to the system is recorded individually and then updated by the node itself. Thus, each node participating in the network operates independently of the other nodes. The blockchain is currently the best known distributed ledger technology (DLT). How this data is distributed, structured and agreed upon (consensus) will dictate the type of DLT (Fig. 2).

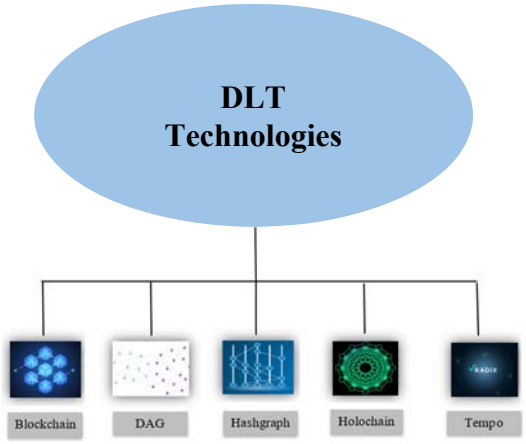

Fig. 2. Type of DLT Technologies

3.1. Blockchain

Blockchain is one of the most popular types of DLT. Blockchain is a type of DLT where transaction records are kept in the ledger in the form of a blockchain. In a blockchain, each block (Fig. 3) is linked to the previous one thanks to the digital signature called here block hash. Each block consists of three important elements: the previous block hash, the timestamp and the transaction data usually presented by a Merkle tree.

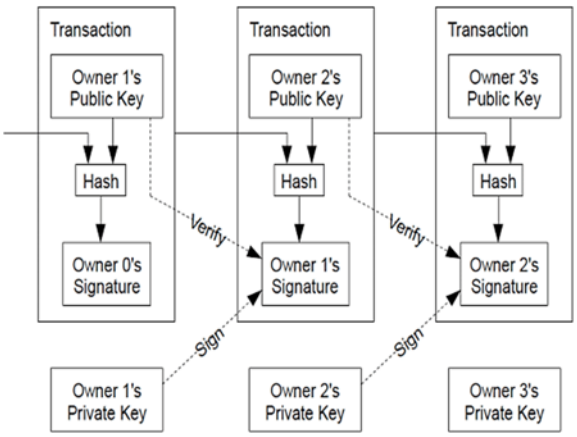

Fig. 3. Block structure.

When there is a new transaction, it is sent to all nodes of the network. The miner nodes authenticate

the transaction using their signature, if the transaction is valid, they mine it in a securely encrypted block. The miner who first succeeds in solving the underlying consensus problem, will then be able to publish his block which will be added to the blockchain. Since then, the transactions contained in this block can no longer be modified. This makes the blockchain a secure system because it is difficult to corrupt. There are several types of blockchain. A blockchain can be private, public or consortium. It can also allow or not the implementation of smart contract.

3.2. DAG

Another ambitious addition to the distributed ledger without the blockchain family is the DAG (Directed Acyclic Graph). A DAG is a particular data structure that allows transactions to be validated and time stamped by interconnecting them to each other unlike the blockchain which groups them together. Even though it is an alternative, the structure of this ledger is really different. One of the main benefits of implementing the DAG distributed ledger is the ability to offer nano transactions at no cost. This is because scalability improves as the network grows. In other words, the more transactions there are on the network, the faster it can settle them. A DAG is much more scalable than a traditional blockchain.

DAG takes a different route to consensus. The distributed ledger system stores transaction processes on nodes. Here, each member of the network is called a "node" just like the blockchain. All nodes in the network validate transactions on the ledger and are also represented by validated transactions. Any node can initiate transactions. However, in order to validate them, it must verify at least two of the previous transactions in the ledger. Once it has validated them, its transaction is confirmed. The more a node validates, the more valid its transactions become in the distributed ledger database.

Thus, if a transaction (Fig. 4) has a longer branch of previously validated transactions, it will have the most weight in the ledger. However, an algorithm will randomly select the two previous transactions for each member to validate. Because if not, members will only validate their transactions and leave another one. This is actually a new form of consensus to achieve greater scalability. Because of this nature of the distributed ledger implementation, companies that need a higher volume of transactions every second should use it.

IOTA [7] is the most popular example of an open source DAG distributed ledger. It is intuitive and scalable, designed to support friction less data and value transfer. IOTA uses quantum robust signatures to protect the network from next generation computing power. It is based on the Tangle [5] witch is a public registry replicated on all nodes. All data in the Tangle are stored in objects called transactions. Once a transaction is attached to the Tangle, it is immutable. All transactions in the Tangle are attached to two others to form a Directed Acyclic Graph (DAG). Each transaction in the graph is represented by a box and each attachment is represented by a line. When a new transaction is attached to the Tangle, it is attached to two previous transactions, adding two new lines to the graph.

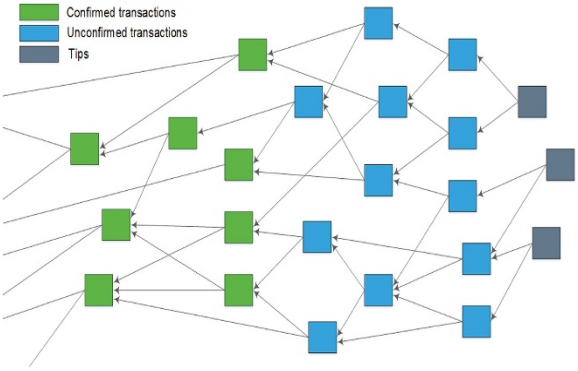

Fig. 4. IOTA transaction [7].

3.3. Hedera Hashgraph

Hedera is a project born in August 2018. It doesn't use a blockchain structure but a particular DAG structure called hashgraph. In the hashgraph [5], all transactions are stored in a parallel structure (Fig. 5).

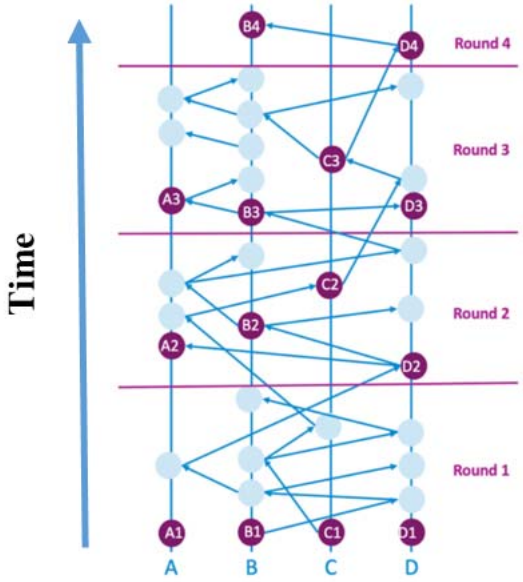

Fig. 5. Hashgraph vote.

Each circle represents a ledger record called an event, which is analogous to a block on a bockchain. An event contains: the timestamp, the transactions, and the hash of the two previous events witch they are joins. All events are therefore linked together irreversibly until the first event of the graph. Hashgraph uses a gossip protocol, the nodes are constantly trying to contact each other in a random way. The gossip algorithm makes the information flow

at a high speed on the network. As all transactions occur on the network, within seconds, everyone on the network will know where the transaction would be placed in the ledger. In addition, everyone on the network will know that the entire network is aware of the existence of the transaction and, therefore, will make changes accordingly.

To validate its transactions, nodes use a virtual voting system. The hashgraph is first divided into several rounds and in each round the nodes will vote to find a consensus on the validity of a transaction and on the timestamp and therefore their order of inscription on the ledger.

3.4. Holochain

In holochain [8], each node or agent maintains a single source string of their transactions, associated with a shared space implemented as a validating, monotonic, sharded Distributed Hash Table (DHT), where each node applies validation rules to the data in the DHT and provides the provenance of the data in the source strings from which it came. A Holochain (Fig. 6) is the set of these three elements: the shared database of public data (DHT), the local hash-chain of private data to an agent (local hash-chain), and a set of common rules (Nucleus).

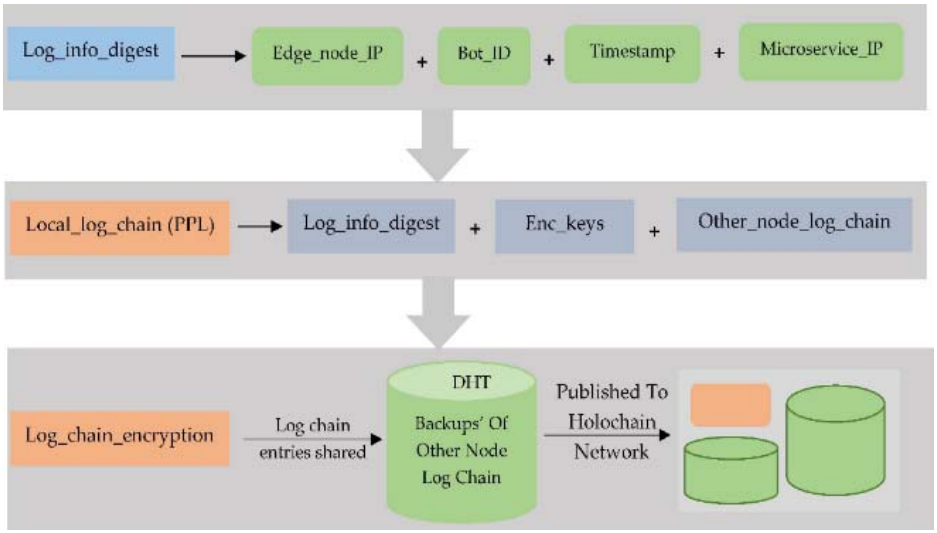

Fig. 6. Holochain's components [8].

Each agent has the common rules of operation: the source code of the distributed application, called Nucleus. By consulting its copy of the Nucleus, the node can check the validity of the information it receives from the other nodes (the signals). Therefore, each node has its own local hash-chain of private data. A node can allow, at its discretion, another node to view its local hash-chain. Also, when a node decides to modify the shared database (DHT), it must first write the information to its local hash-chain and then have it audited by other nodes to see if the addition meets the common rules. Each node decides which private data it wants to share on the common database, so it has sovereignty over its data. Holochain consumes very little energy and will run really well on a phone or small 45 W computer.

3.5. Tempo

The tempo radix distributed ledger database works on three major principles:

- Have a networked cluster of nodes.
- Distributed global ledger among the cluster of nodes. Special algorithms for timestamp events in the ledger.
- Each instance of this distributed ledger database is known as a universe. In the universe, each event is called an "atom".

This is a bit different from other distributed ledger databases on the market. Any node can choose to carry a subset of the entire global ledger with it. The subset of the ledger is called fragments, and each node carrying a fragment will receive a unique identifier for its subset of the ledger. Thus, nodes are not required to carry the burden of the global ledger on the network. This ensures that the network can handle a larger amount of load, increasing scalability. When a node wants to validate transactions, it uses logical clocks to do so. The usual distributed ledger database timestamp is not capable of achieving consensus on its own. This is because of the perspective of time changes from one person to another.

4. Some IoT Security Solutions using DLTs

The Table 2 gives a comparative analysis between the different DLTs, whereas Table 3 lists challenges and opportunities due to certain keys factors.

Table. 2. DLTs comparison table.

DLTs	Applications	Transaction/s	Consensus algorithm	Storage	Scalability	Security	Smart Contract
Blockchain	Bitcoin	About 3	PoW	Important	↓	High	No
	Ethereum	7-15	PoW	Important	↓	High	Yes
	Hyperledger	3000-20000	pBFT	Important	↓	High	Yes
DAG	IOTA	More than 1000	DAG-based consensus	Low	↑	Medium	Yes
	Hashgraph	About 10000	Gossip + virtual vote	Low	↑	Medium	Yes
Holochain	Holochain	About 56000	No general consensus	Low	↑	Medium	Yes
Tempo	Radix	About 1000000	Gossip	Low	↑	Medium	Yes

Table 3. IoT-DLT challenges and opportunities due to certain keys factors.

Key factors	Challenges/Opportunities	
Immature technology, Implementation cost	Absence of widespread adoption Challenges to businesses	**Challenges**
Lack of integration with existing solutions		
Strong encryption mechanisms		
Lack of adaptation of existing regulatory frameworks	Changes needed for adoption across sectors	
Nascent technology	Lack of governance framework	
Multiple non-interoperable implementations	Fragmented ecosystem	
Security vulnerabilities	Challenges for personal data protection	
Distributed systems	High energy consumption	
Need for increased computing power	Associated additional costs	
Legal enforceability of smart contracts	Smart contracts implementation	
Automating processes	Efficiency gains	**Opportunities**
Reducing the need for third-party intermediaries	Cost savings	
Technology adoption	New revenue sources for businesses	
Growth of the ecosystem	Creation of novel business	
Decentralized nature of the technology	Facilitate transactional systems	
Users control their own information	Improve users' trust in carrying out transactions	
Transactions immutability	Reducing the propensity for fraud	
Lack of a central point of failure	More resilient and secure	
Use of public key cryptography	Efficient and cost-effective management of digital identity	
Smart contracts implementation	Smart auditing capabilities	

In [9], the authors propose a data exchange model between owners and consumers based on smart contracts. This model eliminates the trusted third party of traditional centralized systems. Their general data exchange process is performed in eight steps ranging from sharing available information and data of IoT objects via the smart contract, to the payment of rental fees of these data by the consumer. In their proposed model, data owners have control over their data and can authorize access to the data and they can track all transactions since the entire transaction process is transparent and traceable. Their security model meets the criteria of confidentiality, integrity and availability.

The authors of [10] present a holochain-based security and privacy framework for IoT health systems. They point out major setbacks to blockchain related to increasing storage and network size requirements. In the proposed system, patients, doctors, staff, are considered as agents who can actively participate in the network and transfer information. Considering the storage space limitations of IoT objects, they use the cloud to process and store the transaction of a holochain network. The proposed scheme has been analyzed showing the higher efficiency of the holochain compared to rival blockchain systems. They highlight a significant reduction in time and complexity.

In [11], the authors identified the need for fast transaction, IoT network privacy. They have highlighted the main areas of vulnerabilities in the private and public sectors in Dubai in order to propose a sanitary framework. Thus, this one presents an approach using IOTA and Tangle technologies. They discussed the creation of two applications on the Tangle: a smart electricity meter and a smart toll system.

In [12], the authors propose a Lightweight Scalable Blockchain (LSB) optimized for IoT requirements while providing end-to-end security. DTC requires that each head cluster waits a random time before mining, i.e., adding a block instead of solving a computationally demanding headache, which significantly reduces the mining processing overhead. It also offers a distributed debit management (DTM) mechanism to dynamically adjust certain system parameters to ensure that the throughput of the public blockchain does not deviate from the transaction load in the public blockchain network.

DTM ensures that network is self scaling, i.e., as the network grows in size, more transactions can be appended to the public blockchain, thus increasing the throughput. Qualitative analyses have shown that their approach is resistant to several types of attacks [13]. Moreover, simulations have shown that packet overhead and delay are reduced, as the scalability of the blockchain has increased.

In [14], the authors design a new protocol to improve the security of distributed IoT devices. Their solution is essentially based on the hardening of IoT devices. This approach enables secure deployment of IoT devices by reducing the threat of surveillance and theft, while improving operator accountability and trust in IoT technology.

5. Challenges of DLT-IoT Integration

Table 2 gives a comparative analysis between the different DLTs studied here. In this table, pBFT (Practical Byzantine Fault Tolerance) is a consensus algorithm for enterprise consortiums where members are partially trusted. Whereas, Proof-of-work (PoW) is a well-known decentralized consensus mechanism. As we can see, this table gives an overview of some important characteristics of DLTs.

The security aspect of DLTs, and in particular of blockchain, justifies the attraction of researchers to address the security challenges of the Internet of Things. With the presence of smart contracts, several scenarios can be realized.

The convergence of IoT and a DLT such as blockchain still presents many challenges that need to be addressed in order to take full advantage of the benefits offered by DLTs [15].

There is not yet a reference model for the integration of IoT and DLTs. However, there are primarily two ways of integration:

- **Tight integration:** In this type of integration all IoT devices are considered as peers of the blockchain. All IoT communications are recorded in the blockchain.
- **Loose integration:** In this type of integration, only resource-rich IoT devices are considered peers of the blockchain. Other devices can communicate with the blockchain through these intermediaries.

The choice between these two types of integration depends on the level of security required but also on the characteristics of the connected devices.

The tight integration offers more advantages in terms of security. All exchanges are recorded in the blockchain and therefore verified and approved by all the nodes. This system provides security services such as non-repudiation.

However, this approach increases storage requirements and may not be feasible for some use cases. In contrast, loose integration allows the blockchain to be used to perform only certain interactions. DLT-IoT integration presents some challenges:

- **Storage:** one of the major problems of this convergence is the great difference in storage space requirements of the blockchain and paradoxically the limitations of connected objects.
- **Computing power:** participation in the blockchain consensus requires a certain amount of computing power and most connected objects do not have this computing power.
- **Scalability:** connected objects tend to produce and exchange a lot of data, and with tight integration, the number of transactions in the blockchain can increase rapidly and may cause the blockchain to slow down.

Nevertheless, despite these major challenges, the use of DLT brings many advantages and opportunities as we can see in table 3 which assesses challenges and opportunities due to certain keys factors. Finally, the table 4 summarizes the advantages and challenges of this convergence.

Table. 4. Benefits and Deficiencies DLT-IoT paradigm

<table>
<tr><th colspan="2">DLT-IoT paradigm</th></tr>
<tr><th colspan="2">Main features</th></tr>
<tr><td colspan="2">– An immutable record
– Disintermediation
– A lack of central control by one party
– New opportunities (Table 3)
– Tight integration
– Loose integration</td></tr>
<tr><th>Benefits</th><th>Deficiencies</th></tr>
<tr><td>Security</td><td rowspan="2">Scalability</td></tr>
<tr><td>Decentralization</td></tr>
<tr><td>Improved interoperability</td><td rowspan="2">Storage</td></tr>
<tr><td>Greater resilience</td></tr>
<tr><td>Greater privacy</td><td rowspan="2">Computing Power</td></tr>
<tr><td>Fault tolerance</td></tr>
</table>

6. Conclusion

In this study, we have presented the existing DLTs and made a comparison according to different parameters. This study is intended to provide additional support to help in the choice of DLTs for IoT applications. Many recent works on IoT has shown that the convergence of these two technologies, although very different, provides several solutions to the challenges of IoT, especially for security.

Thus, the key features of DLT-IoT are associated with its decentralized nature. In DLT-IoT, multiple copies of information are held by different connected objects, with data updating process by consensus and without the need for a third party. As a result, DLT-IoT can offer more efficiency, gains in trust and data reconciliation across all participant nodes. This means that DLT-IoT is able to provide:

– An immutable record. Data added is in theory unchangeable and secure, with the agreement of all participants as to the contents.
– Disintermediation. Direct nodes interaction, without the need for a third party.
– A lack of central control by one party. Changes are decided on a consensus basis by multiple connected participants.
– New opportunities for management and sharing of data and many others, such as, more efficiency, costs savings, more resiliency and security with reduction of the propensity for fraud.

However, some of the major problems of this convergence are the great difference in storage and computing power requirements of blockchain and paradoxically the limitations of connected objects.

Finally, in order to fully benefit from the advantages of DLTs, it is needed to find ways to circumvent the limitations of connected objects in order to set up a good integration architecture for these two technologies.

References

[1]. Ore Ndiaye Diedhiou, Cherif Diallo, An IoT mutual authentication scheme based on PUF and blockchain, in *Proceeding of the IEEE International Conference on Computational Science and Computational Intelligence (CSCI),* Las Vegas, USA, 2020, pp. 1034 – 1040.

[2]. Cherif Diallo, Security Issues and Solutions related to Data Aggregation Process in WSN, *International Journal of Computer Science and Network Security,* Vol. 17 No. 4, April 2017, pp. 59-71.

[3]. Goyal, S, Public vs private vs hybrid vs community-cloud computing: a critical review, *International Journal of Computer Network and Information Security,* 6, 3, 2014, pp. 20-29.

[4]. Xiong, Z., Zhang, Y., Luong, N. C., Niyato, D., Wang, P., & Guizani, N. The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things, *IEEE Network,* 34, 1, 2020, pp. 166-173.

[5]. Schueffel, Patrick, Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph - A HighLevel Overview and Comparison, *SSRN Electronic Journal,* 2018, https://ssrn.com/abstract=3144241

[6]. Farahani, Bahar Firouzi, Farshad Luecking, Marku, The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions, in *Journal of Network and Computer Applications,* Vol. 177, 2021, p. 102936.

[7]. IOTA Web site (https://www.iota.org).

[8]. Eric Harris Braun, Nicolas Luck, Arthur Brock, Holochain, scalable agent-centric distributed computing DRAFT(ALPHA 1) – 2/15/2018..

[9]. Pham, Hoang Anh Le, Trung Kien Pham, Thi Ngoc My Nguyen, Hoai Quoc Trung Le, Thanh Van, Enhanced Security of IoT Data Sharing Management by Smart Contracts and Blockchain, in *Proceedings of the 19th International Symposium on Communications and Information Technologies (ISCIT' 2019)*, 2019, pp. 398 – 403.

[10]. Zaman, Shakila Khandaker, Muhammad R. A. Khan, Risala T. Tariq, Faisal Wong, Kai-Kit, Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare, *IEEE Internet of Things Journal*, arXiv:2103.01322.

[11]. Shabandri, Bilal Maheshwari, Piyush, Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle, in *Proceedings of the 6th International Conference on Signal Processing*

and Integrated Networks (SPIN 2019), 2019, pp. 1069 - 1075.
[12]. Dorri, Ali Kanhere, Salil S.Jurdak, Raja Gauravaram, Praveen, LSB: A Lightweight Scalable Blockchain for IoT security and anonymity, *Journal of Parallel and Distributed Computing,* 134, 2019, pp. 180–197.
[13]. Anuska Gupta, Bhumika Gupta, Kamal Kumar Gola, Blockchain technology for security and privacy issues in internet of things, *International Journal of Scientific and Technology Research,* 9, 3, 2020, pp. 377-383.
[14]. John Wickstrom, Magnus Westerlund, Goran Pulkkis, Rethinking IoT Security: A Protocol Based on Blockchain Smart Contracts for Secure and Automated IoT Deployments, *arXiv:2007.02652,* 2020.
[15]. Advait Deshpande, Katherine Stewart, Louise Lepetit, Salil Gunashekar, Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards, Overview Report, *British Standards Institution (BSI),* 2017.