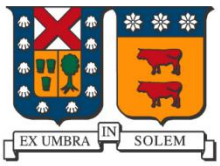
UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA

DEPARTAMENTO DE INDUSTRIAS

PROGRAMA DE DOBLE TÍTULO





UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Blockchain and beyond, integration of IoT devices with the distributed ledger technology

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL INDUSTRIAL

Profesor Guía

Rafael Favereau U.

Profesor Correferente

Oscar Saavedra

Candidato

Antonio Andrés Martínez Ulloa

Diciembre 2020

Author's comments and acknowledgments

Many times, society guides us along a certain path. Since we start the education system at an early age, they teach us to be responsible, organized, to study, and try to stand out from others. Our performance is assigned with a qualification, then the cycle continues in the university and later at the work. The above is important, it is necessary to forge discipline and set goals to achieve things. However, we should not lose our dreams or creativity by pursuing objectives set by others such as good grades.

For trying to get the best position in a professional career, the best university, or the best job, we stop pursuing our dreams. Those "best positions" have been cataloged as such by other people who do not necessarily have our tastes and preferences. In the end, in the race to try to excel and be different, we do not realize that we end up the same as the rest, working day by day but to fulfill the objectives of others while forgetting ours. I've heard older people tell or regret how they spend their lives doing things that do not make them grow as a person or feel fulfilled, constantly thinking that the future will be better, but not taking advantage of the present.

From my young perspective of life, those who achieve self-realization are those who pursue their goals, whether they are their own or common, but strive to achieve them. My first objective has already been set: to be free in time and be able to decide what to do day to day.

The university is just an academic institution that gives you tools to work. However, the university of life is much harder to pass, the older we become, the more we care about unimportant things. When we are children, we laugh and celebrate more easily, we see life from a much simpler perspective and enjoy it without hesitation.

Sometimes we get obfuscated by things as simple as a qualification or a job interview, however, when that happens, it is because we forget in another part of the world there is a barefoot child who walks miles to find water, another who does so to be able to go to the school and another that escapes the war that has come to his city.

My thanks are to life, which has given me many opportunities that others do not possess, and yet many manage to be happy in much more adverse conditions.

"…nos hablaron una vez cuando niños, cuando la vida se muestra entera, que el futuro, que cuando grandes, ahí murieron ya los momentos…"

E. Gatti

Abstract

Blockchain is a fully distributed system that stores a consistent and immutable linear event log of transactions between networked actors (1). In simple words, it is a digital and distributed database that links blocks of information securely and transparently, where there is no need for a central authority since it is governed by any peer that wants to join the network. If it unfolds in the right way, blockchain technology has the potential to revolutionize electronic transactions, in the same way, as in its time did the internet in communications.

In this research work, the potential of the blockchain integration with the Internet of Things (IoT)[1], the adoption of IoT devices in the industry, as well as other distributed ledger alternatives for an IoT ecosystem are analyzed.

Blockchain was born as a digital ledger to support a reliable and secure decentralized payment network (P2P) (2). However, just as in the past it happened with the internet, the potential of blockchain technology has been discovered and developed over recent years, and now can support much more complex operations than a payment network. Among the new developments of this technology, there are blockchain protocols intended for the use of autonomous organizations, digital governance, decentralized applications, smart contracts, interoperability among many other aspects.
It is in the development of these new blockchains protocols, that countless additional possibilities arise, such as the use of the blockchain in an Internet of Things network. In the world of the Internet of Things, there is a huge range of use cases such as smart cities, smart grid, smart homes, connected cars, smart farming, supply chain, etc. However, to achieve such interconnectivity of the devices, a network capable of supporting the transmission of data in a safe and reliable manner is necessary. Most of the network structures of current IoT devices are based on centralized networks, where the single point of failure[2] problem is present.

Identifying the value proposition and limitations that the blockchain technology offers compared to traditional service providers allows discovering which business models can be challenged by the use of this technology (e.g. notary, financial industry) (1). However, this investigative work does not limit itself to looking for an established business in which the blockchain can help or improve a current technology or process, it also investigates new business opportunities that may arise through blockchain-based applications.

[1] Internet of Things is the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

[2] A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working.

Sommario

La blockchain è nata come un registro digitale per supportare una rete di pagamento decentralizzata, sicura ed affidabile. Si tratta di un sistema distribuito che immagazzina un registro consistente ed immutabile di eventi lineari delle transazioni tra attori in rete. In altre parole, si può definire la blockchain come un database digitale che collega blocchi di informazioni in modo sicuro e trasparente e ha il potenziale per rivoluzionare le transazioni elettroniche.

In questa ricerca vengono analizzati lo studio della integrazione delle Internet of Things (IoT) con la blockchain, le sfide che ciò comporta e l'adozione dei dispositivi per l'utilizzo nelle industrie così come altre alternative dei *distributed ledger* per l'IoT.

Proprio com'è successo con internet nel passato, il potenziale della tecnologia blockchain è stata scoperta e sviluppata negli ultimi anni per supportare operazioni più complesse delle semplici transazioni in rete. Tra i nuovi sviluppi di questa tecnologia ci sono protocolli di blockchain destinati all'uso di organizzazioni autonome, governance digitale, applicazioni decentralizzate, contratti intelligenti, interoperabilità e altri aspetti.

Lungo il percorso di sviluppo dei più recenti protocolli di blockchain sorgono innumerevoli possibilità aggiuntive per l'uso della tecnologia stessa, come nel caso dell'utilizzo della blockchain su una rete di IoT. Del mondo delle IoT si può trovare un potenziale utilizzo in città intelligenti, case intelligenti, automobili connesse, agricoltura intelligente, e altre ancora. Inoltre, si ha bisogno di una rete capace di supportare le trasmissioni di dati in modo sicuro ed affidabile per ottenere l'interconnettività richiesta dai dispositivi. Le strutture di rete degli attuali dispositivi IoT si basano su reti centralizzate, in cui è presente il problema del singolo punto di errore.

L'identificazione della *value proposition* e dei limiti che la tecnologia blockchain offre rispetto ai fornitori di servizi tradizionali permette di scoprire quali modelli di business siano capaci di superare le diverse sfide che sorgono dall'uso di questa tecnologia, ad esempio il settore finanziario oppure notarile. Tuttavia, l'analisi di questo studio non si limita a cercare le migliorie portate dalla tecnologia blockchain a un'azienda tradizionale, ma cerca anche di prevedere le potenziali opportunità di business che potrebbero sorgere in funzione delle applicazioni quotidiane della tecnologia blockchain.

Executive Summary

This research work searches the current scientific literature about the development of blockchain technology as well as IoT device networks. The blockchain technology offers the features that a robust IoT network requires such as security, trust, and reliability, but since both are relatively new technological concepts (2) (3), they still present many challenges that must be solved to develop the maximum potential of each (4) (5) (6) (7) (8). This motivated the present study that analyzes the potential of the inclusion of blockchain technology in networks of IoT devices, analyzing the challenges and advantages that this entails.

The objective of the research work is to analyze, through the review of the state-of-the-art scientific literature, that the use of blockchain technology, as well as other forms of distributed ledgers, have the potential to solve the general problems that the current IoT networks present, such as the lack of security and reliability in the transmitted data.

For the Review of the state-of-the-art scientific literature, various sources of information were used as peer-reviewed articles for the classification of architectures and definitions of the research field, as well as independent research papers and reports to cover a field of research broader in the IoT-blockchain spectrum. As complementary sources, digital media specialized in blockchain technology as well as electronic newspapers were used. Regarding the methodology of data selection, research articles from the last three years (2017, 2018, and 2019) were preferably used as they present the clearest and most advanced definitions and use of cases regarding the development of blockchain technology.

The potential solution of an IoT network enhanced by blockchain it is exposed as an IoT-blockchain ecosystem, which can work by adopting the blockchain to transmit and store all network information or use it partially to improve certain specific aspects of it (5). The advantages and benefits that blockchain technology can bring to an Internet of Things network as security (9), identity (10), autonomy (11), reliability (5), e-governance (12), among others, as well as the challenges that the above involves, are analyzed. The research work has been developed as follows:

First, the fundamental notions and concepts of blockchain technology for understanding subsequent chapters are presented. To facilitate understanding, a first approach is made with a database, analyzing the similarities between both structures and their differences. Later, similar work is carried out but concerning an Internet of Things (IoT) environment. The architecture and standards of an IoT system together with the strengths of each are explained. Subsequently, the current applications of the IoT that are developed in the industry (without considering the use of blockchain) are

introduced, as well as its main challenges and restrictions to maintain exponential growth like the one it experiences. The IoT chapter ends with a global market analysis of the IoT environment in both people and industry, the growth it has had over these years, and its projections.

Afterward, a blockchain of things is presented as an IoT ecosystem strengthened with blockchain technology. The need to increase some aspects of IoT networks such as their security, confidentiality, availability, and the dangers that an insecure network represents are analyzed with cases of attacks and theft of information in IoT networks. Different types of architecture are then presented for an IoT-blockchain ecosystem as well as, two proposed use cases (13). Cases of industry development in IoT networks (14) along with the use of blockchain and the advantages are also shown. However, to achieve a blockchain of things ecosystem, several challenges must be resolved. The blockchain challenges section highlights the current problems that technology must overcome to complement an IoT network such as low energy use, scalability, interoperability, among others.

Presented de challenges, the current solutions that are being developed in each aspect as on-chain solutions, off-chain solutions, and consensus mechanisms adapted for IoT are presented. The above proposals have the potential to solve the problems of the blockchain itself and also maintain the benefits of the blockchain (scalability or interoperability), however, they are developments that are still in their early stages.

Case study – Chainlink: an additional problem and external to the blockchain arises. How to ensure that the data entering the blockchain is reliable. In this chapter, a case study of a company that is developing a solution to this problem is carried out (15). Chainlink presents a structure to decentralize information before it enters the blockchain, increasing its reliability as well as providing interoperability of the information sources that enter data into the blockchain.

Case Study – IOTA: C*hapter 7* introduces IOTA, a company that is developing a type of distributed ledger technology (DLT) designed specifically for use in an IoT network (16). The IOTA proposal seeks to maintain the same benefits of the blockchain but with a different architecture. This proposal starts with fewer problems than the blockchain, being a network in theory, infinitely scalable but presents other problems that must also be faced for the integration of all types of IoT devices.

The research work concludes that, although the technological development of an IoT-blockchain ecosystem is still at an early stage, solutions to the challenges encountered are being developed, giving to the blockchain technology the potential to be an ideal and necessary complement to an IoT

ecosystem and thus be able to maximize the potential of a safe, reliable and decentralized IoT ecosystem.

Data selection

Google Scholar web search engine, that indexes metadata of scholarly literature, reveals that the scientific literature that contains exactly the words "blockchain" and "Internet of Things" in the title of the article (also considering "IoT") results in 516 scientific articles, of which 380 (74%) were published from 2018 and 210 (41%) during 2019, the year of completion of this research work. The same goes for more specific search engines such as IEEE Xplore or ScienceDirect where the largest number of publications is concentrated in recent years and increasingly. Considering that 41% of all publications have been made during this year and only until August, it can be induced that research in the area of IoT is an increasingly studied topic.

For the review of the state-of-the-art scientific literature in the blockchain intended to support IoT networks as well as general blockchain and IoT articles, heterogeneous sources of information were used and will be detailed below.

Primary data sources: they were used for the realization of the diagrams, graphics, and IoT-blockchain architectures presented. Peer-reviewed sources, mainly from IEEE Access Journal, were used for the presentation of the use cases of the use of blockchain in an IoT network.

Secondary data sources: in this category, papers presented at conferences were used, as well as papers by researchers from different universities but without publication of articles in scientific journals. This literature was used to internalize about many aspects related to blockchain and IoT as well as discover other scientific articles related and cited by these sources.

Tertiary data sources: in this category, newspapers were used as a source of news data related to attacks on IoT networks, as well as digital media specialized in the field of blockchains such as *Cointelegraph.com* and *Coindesk.com* related to the use of blockchain in the IoT field. Online publishing platforms as *Medium.com* were also used, where it is possible to obtain first-hand information related to the latest developments of blockchain technology. Particularly in this platform, writers representing important technology companies, project leaders as co-founders & CEOs of blockchains projects, as well as project developers or freelancers are found. In these places is the information related to the latest advances and technological developments as far as blockchain is concerned.

Other sources of data: a report of the IoT development in the industry, of the Vodafone group, as well as blogs from companies involved in the development of blockchains projects such as IBM, Linux Foundation, Microsoft, Santander Bank, were also used, to name a few.

Summary of methodology

The research work is based on a review of the state-of-the-art scientific literature in mainly three fields.

- Blockchain technology and its derivatives
- Internet of Things
- Blockchain applied to the Internet of Things

The methodology used was as follows:
Given that blockchain technology is a relatively recent technological development, the initial step was to confirm that the chosen topic had sufficient literature and articles available to support the research. Subsequently, a selection of about 80 scientific articles was made that related to either the use of the blockchain and IoT environments jointly or the study of the topics separately. These articles were used for the development and presentation of both topics in detail (their architecture, operation, strengths, and weaknesses).

With the reading of these scientific articles, the most important ones were selected and used (about 26 articles of those initially found). A common pattern was found, older articles (2016 or earlier) focused on general aspects of blockchain technology while their relationship with IoT environments was very general and poor. Given the above, the research focused on recent scientific articles (2017, 2018, and 2019) since it is more specific in terms of the use of blockchain in IoT environments. From these articles as well as those rejected, other referenced research projects or works were discovered that were studied in more detail given their usefulness with the topics studied. These articles, where several have been published in journals peer-reviewed, served as a structural basis for the research work.

As a complement and last-minute data sources, publishing platforms were used as first sources of information, since the origin comes directly from the developers who are developing the technology. This mechanism was widely used in *Chapters 4* and *5*, where the developers or members of different blockchain projects, exposed the challenges that blockchain presents as well as the solutions that are being developed.

For the case studies, the technical information provided by the companies, such as their Whitepapers, was used, as well as official information on their web pages.

Table of Contents

1 Conceptual Background 4

1.1 Introduction 4

1.2 What is a blockchain 4

1.3 Blockchain or traditional distributed database 5

1.4 Blockchain compared to traditional databases 6

1.5 Blockchain compared to distributed databases 7

1.6 Blockchain design 10

1.7 Characteristics of a blockchain 10

1.8 Types of blockchain 11

1.9 Public blockchain 11

1.10 Private blockchain 12

1.11 Permissionless and permissioned, a detailed approach 12

1.12 Decentralization 14

1.13 Consensus algorithm 15

1.14 Soft fork versus hard fork 17

1.15 Smarts contracts 18

1.16 Smart contracts challenges 19

2 Internet of Things 20

2.1 Internet of Things architecture 22

2.2 Types of IoT architectures & standards 23

2.3 IoT applications 26

2.4 IoT devices constraints & challenges 28

2.5 Market integration and prospective 29

2.6 Industry perspective 31

3 Blockchain of things 34

3.1 Use cases 38

3.2 Security and privacy scandals 39

3.3 Incorporating blockchain into IoT security 43

3.4 Types of IoT architectures enhanced with blockchain 45

3.5 Blockchain case of use for firmware detection 46

3.6 Blockchain case of use for dataset identification 48

3.7 IoT-blockchain initiatives at the industry 49
4 Blockchain challenges 51
4.1 Energy efficiency 51
4.2 Scalability 51
4.3 End-to-end reliability 52
4.4 Interoperability 53
4.5 Connectivity 54
4.6 Oracles: A point of failure 55
5 Solutions 56
5.1 First layer solutions 58
5.2 Second layer solutions 58
5.3 Consensus mechanisms for IoT 59
5.4 DLT alternatives for IoT 61
5.5 Interoperability 61
6 Case study - Chainlink 62
6.1 Freeloading problem 65
6.2 Off-chain aggregation phase 65
6.3 Operation Example 66
6.4 Conclusion of the case study 67
7 Case Study - IOTA 68
7.1 Tangle's architecture 68
7.2 Strengths 70
7.3 The centralized coordinator problem 71
7.4 Conclusion of the case study 72
8 Conclusion 72
9 Bibliography 74

List of Figures

Figure 1-1 Database with a Client/Server architecture....6
Figure 1-2 Flow diagram for deciding when to use blockchain in an IoT application....8
Figure 1-3 A blockchain design....11
Figure 1-4 Different projects classified with the detailed approach....14
Figure 1-5 Representation of a blockchain connected with an oracle....20
Figure 2-1 Basic IoT architecture by components based on cloud computing....22
Figure 2-2 IoT architecture by layers....23
Figure 2-3 IoT architecture breakdown by layers and components....23
Figure 2-4 IoT-based architectures....25
Figure 2-5 Some IoT applications....26
Figure 2-6 Global market IoT forecast IoT analytics research 2018....30
Figure 2-7 IoT adoption over the next 10 years....31
Figure 2-8 Percentage of adoption by the number of devices....32
Figure 2-9 Concerns and barriers to adopt IoT of organizations....33
Figure 3-1 IoT in a manufacturing industry....35
Figure 3-2 Scheme of a blockchain storing data from an IoT network.....40
Figure 3-3 Centralized and decentralized systems in IoT architecture....45
Figure 3-4 IoT and blockchain ecosystem, possible interactions....46
Figure 3-5 Blockchain-based compromised firmware detection and self-healing....47
Figure 3-6 Blockchain-based management of membership and reference integrity....48
Figure 4-1 Scalability trilemma....52
Figure 4-2 End-to-end reliability representation....53
Figure 5-1 DLT-based networks scaling solutions....57
Figure 6-1 The behavior of an ideal oracle....64
Figure 6-2 Two-level distribution scenario....65
Figure 7-1 Representation of the Tangle....69
Figure 7-2 Tangle with conflicting transactions present....70

List of Tables

Table 1-1: A Basic database design....5
Table 1-2 Key differences between a blockchain and a database....9
Table 1-3 Advantages between a blockchain and a traditional database....10
Table 1-4 Detailed approach of types of blockchains....14
Table 2-1 IoT estimations (46)....31
Table 3-1 General blockchain technology contributions to an IoT network....37
Table 3-2 Some IoT-blockchain current use cases applied by companies....39

1 Conceptual Background

1.1 Introduction

October 31st, 2008 Satoshi Nakamoto published his famous white paper describing the first known cryptocurrency: Bitcoin. The technology behind this cryptocurrency is the blockchain, and ten years later, the main companies of the world of diverse areas are exploring its implementation (Microsoft, Amazon, Ford, Samsung, Toyota, Walmart, JPMorgan, AXA, Bank of America, Santander Bank, among others).

Blockchain is commonly understood as a disruptive technology that will have to change the industry, but still, the possibilities and cases of use are being discovered in the different sectors of the industry. In the first years, the first great possibility of the development of the blockchain was seen as a truly-free economic network with transactions based on its unique technological characteristics (17). The above is not surprising, given the vision of the blockchain creator, still unknown, Satoshi Nakamoto as published in his famous white book: Bitcoin: A Peer-to-Peer Electronic Cash System. For him, Bitcoin together with the network that supported it, the blockchain, would constitute a purely peer-to-peer version of electronic cash would allow online payments to be sent from one party to another without going through a financial institution (2). However, as the years go by, the potential of blockchain technology has been discovered to work beyond a payment system. Blockchain has been developing to be implemented in different sectors of the industry as well as new business niches.

1.2 What is a blockchain

In its generic form, blockchain technology refers to a fully distributed system for cryptographically capturing and storing a consistent, immutable, linear event log of transactions between networked actors (1). At a basic level, blockchain is a chain of blocks. Digital data is stored (in the "block") and connected in a pubic database ("the chain"). Blockchain is a specific case of distributed ledger, which refers to a ledger spread across the network where every peer holds a copy of the complete ledger. At this point, it is noticed that a blockchain has several similarities with a database, and indeed they do.

In essence, blockchain is a database (with particular characteristics), but a database is not necessarily a blockchain. A database likewise stores information in data structures called tables while a blockchain stores the data in the so-called blocks. Both store information but the design and their purpose are different. A blockchain is a distributed and decentralized database. While in a traditional database, the data may or may not be distributed, its management is centralized.

1.3 Blockchain or traditional distributed database

In a nutshell, a distributed database means that there are two or more files located on different sites. **However, one of the blockchain innovations is that they integrate a consensus mechanism, which gives the network decentralization in terms of control and not only in terms of distribution of the data**. In a blockchain, we can protect ownership of data individually without the need of being managed by a centralized entity. Distributed database systems rarely have to solve the Byzantine Generals Problem (explained later in section *1.13 Consensus algorithm*), since there is a central point of control (or a small number of trusted participants) that coordinates the whole system.

In the most general sense, a database is an organized collection of data belonging to the same context and systematically stored for later use. It started as a flat-file hierarchical system to provide data gathering and storage. Nowadays there are applications called database management systems (DBMS) that allow you to store and subsequently access the data quickly and structured being possible also to use relational models allowing more complex ways of data gathering, relating information between multiple databases. A database is not encrypted by default and permissioned (only some actors can intervene), records can also be modified. In the following figure, a representation of a basic database is shown.

A column stores data in a field

A row is called a record

ID	Name	Address	Phone
1000	Satoshi Nakamoto	Unknown	666-777-888
1001	Andreas Antonopoulos	Decentralized Square	666-777-888
1002	Julian Assange	9 John Sessions Square	666-777-888

Table 1-1: A Basic database design

Database Architecture

Databases can be managed by different types of database management systems (DBMS). Next, a client-server architecture, one of the most traditional and simple types of a DBMS, will be presented. In this type of DBMS to access the information or write data, clients need to connect to the server. The control over it with the capability to create, read, update, and delete is done by the administrator who is also in charge of allowing access and give permissions. The client software is in charge of establishing a secure connection and ask for access. Thus, the client should be authenticated before having access to the database. A simplified architecture of a

Client/Server structure would be the following: the database is attached to a server (database server) and the database server hosts the database management system and provides it to other computers. Client computers access the databases on the server via front-end[3] interface or an API[4] in a client installed the application. In *Figure 1-1* a graphic representation of a Client/Server system is represented.

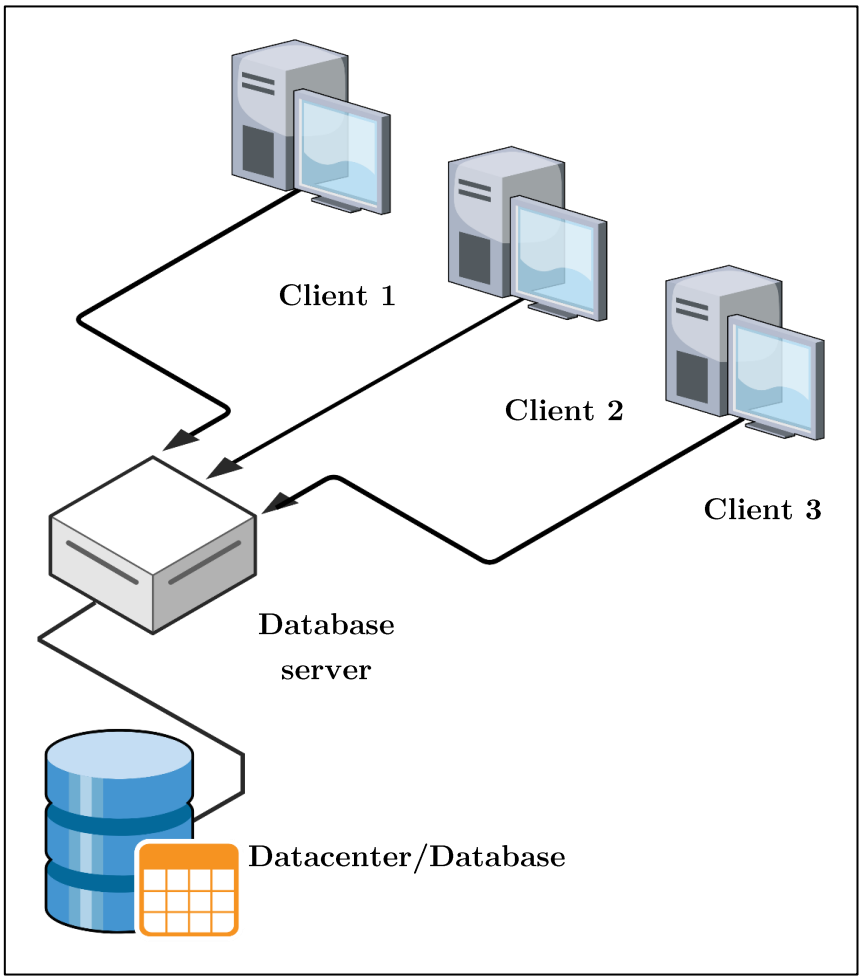


Figure 1-1 Database with a Client/Server architecture

1.4 Blockchain compared to traditional databases

Depending on the system requirements, it will depend on whether it is convenient to use a database or a blockchain. In general, most data systems use a centralized structure in all aspects (control and storage of information). The control given the centralization of a database gives it the speed and a certain degree of confidentiality (depending on the security system used). However, a decentralized structure such as the blockchain allows information to be distributed in such a way that it is stored in many nodes at the same time, so the attacker should not only focus on controlling a system or the central entity that owns the information but rather a series of nodes that

[3] The front-end is an abstraction, simplifying the underlying component by providing a user-friendly interface.
[4] The application programming interface (API), is a set of subroutines, functions and procedures (or methods, in object-oriented programming) that offers a certain library to be used by other software as an abstraction layer.

have an exact copy of the information. On the other hand, if you need to enter and delete records, a database is still an ideal alternative, given the ease of modifying information. Not all systems require storing a large amount of data for a long time, so if deleting them is a necessity, a traditional database also represents a better alternative.

1.5 Blockchain compared to distributed databases

In addition to traditional centralized database management systems, there are those that distribute information at different points and not only on a central server, the DDBMS.

Distributed database management systems (DDBMS) have a system where for data storage, they use interconnected nodes. Thus, the distributed network has a central logical point of control that controls and supervises operations, while information is stored at different points. **Server administrators have full control over the operations carried out in these storage points**. Whereas distributed databases only distribute the data across a network, blockchains take this to the next level by giving a decentralized control. Since distributed databases allow secure handling of read-write operation and administrators usually have full control can perform modify or delete operations on the data and its structure.

Blockchains, on the other hand, even with administrative rights, do not have provisions for changing or deletion of data. They are write-only. Every block of data in blockchains links to the next block. Therefore, to make any changes in the data, the root node, as well as all the subsequent nodes, will have to be updated as each of them is linked to the previous one. The above gives the blockchain the property of **immutability.**

Figure 1-2 shows a generic flow diagram that allows for determining the type of blockchain that is necessary depending on the characteristics of an IoT system. The next figure is a generic flow diagram developed by T.Fernández and P.Fraga (18). It indicates if it is necessary to use a blockchain against the option of a database. Also, depending on how much control is needed over the IoT devices (nodes), and how the permissions of the participating nodes are granted, a distinction will be made between the different types of blockchain.

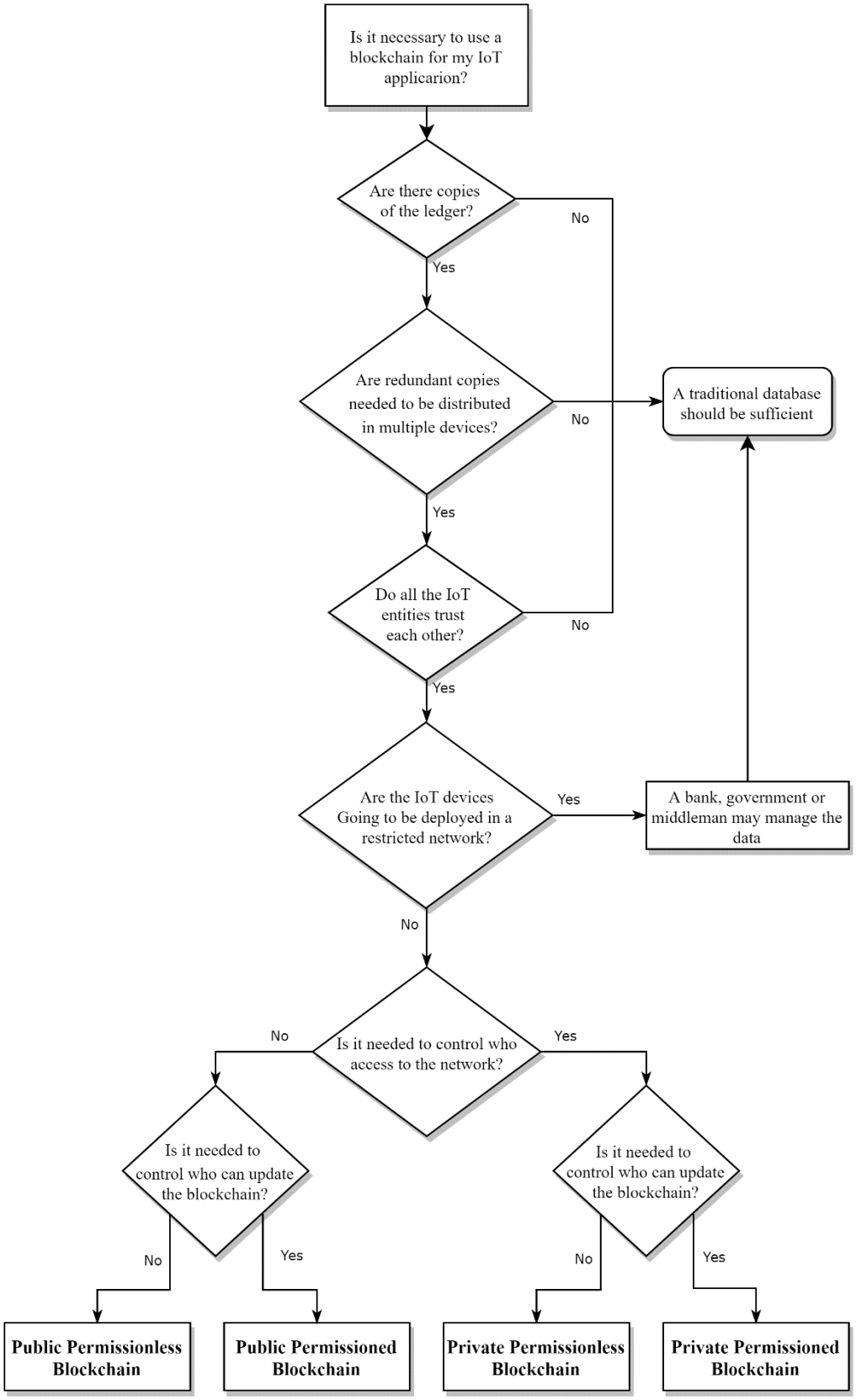


Figure 1-2 Flow diagram for deciding when to use blockchain in an IoT application (18)

As is can be seen, not in all cases a blockchain is needed, in many cases an IoT device network can work with a traditional database structure, depending on whether there are many actors in the network and if there is trust between them. However, an essential point is that traditional and centralized systems will always tend to be more insecure than a decentralized one, as will be explained later given the single point of failure of them. The differences between private, public, permissionless, and permissioned blockchain will be detailed later in *section 1.8 Types of blockchain*. In *Table 1-2,* the main differences between a database and a blockchain are highlighted.

	Blockchain	Traditional Database
Operations	Only insert operation	Create, read, update and delete
Replication	Full replication of block on every peer	Master – Multi-master
Consensus	The majority of peers agree on the outcome of transactions	Distributed transactions (2 phase commit)
Variants	Anybody can validate transactions	Integrity constraints
Disintermediation	Decentralized & distributed trust	Centralized
Confidentiality	Write-controlled	Read and write-controlled
Robustness & security	No individual node[5] is crucial, extreme fault tolerance capability.	The data server is crucial. Security and trust in the centralized system.
Access	Permissionless (public blockchain)	Permissioned, controlled by an administrator

Table 1-2 Key differences between a blockchain and a database

To finalize the comparison, the advantages of each are summarized in *Table 1-3*

Characteristics	Advantage
Disintermediation	Blockchain

[5] Simply put, a network node is a point where a message can be created, received, or transmitted. Usually, a node consists of a physical network device, but there are some specific cases where virtual nodes are used.

Confidentiality	Centralized databases
Robustness	Blockchains
Performance	Centralized databases
History of itself – Audit trail	Blockchains

Table 1-3 Advantages between a blockchain and a traditional database

1.6 Blockchain design

As said before, blockchain stores data in blocks. These blocks have uniform size and contain data, the hash[6] of the block, and the hashed information from the previous block to provide cryptographic security. Data stored inside a block depends on the type of blockchain.

The blockchain database is not stored in any single location, meaning the records it keeps are truly public and easily verifiable (at least in the case of public blockchains). Transactions are broadcast, and every node is creating its own updated version of events. This is what makes blockchain so useful, it does not need a trusted party to facilitate transactions or relationships because the information is reliable by itself. Falsifying a single record would mean falsifying the entire chain in millions of instances so it is virtually impossible if the blockchain is enough decentralized. When data is written in blockchain, it is like etching the data into stone. The information is immutable over time, so it is tamper-proof and reliable since all the nodes are constantly checking the immutability of the blocks. This way, the need for a third trusted party is eliminated (for example, making money transactions without a central entity such as a bank).

1.7 Characteristics of a blockchain

Below, a list of the main characteristics of the blockchain is presented. It is important to mention that these characteristics are valid for a public blockchain, while not all of them are equally valid for a private blockchain. The differences will be detailed in the next section.

- Peer-to-peer: no central authority is needed.
- Distributed & decentralized: ledger spread across the nodes to tamper information is more difficult the more decentralized is the network.
- Cryptographically secured: data is encrypted with different algorithms depending on the blockchain.
- Consensus: blockchain has the capability to update itself and take decisions according to a group of peers, so control of the chain is not conducted by a central authority but by many actors.

[6] A hash identifies a block with a unique id, which also contains the data stored in the block. It is a function that transform data of any size onto data of a fixed size.

- Add-only: data can only be added with time-sequential order, is a non-recursive append-only.
- A blockchain is immutable, so no one can alter the data it contains.
- A blockchain is transparent, so anyone can track the data if they want to.

Figure 1-3 below graphically represents a blockchain and how they are joined by the hash function.

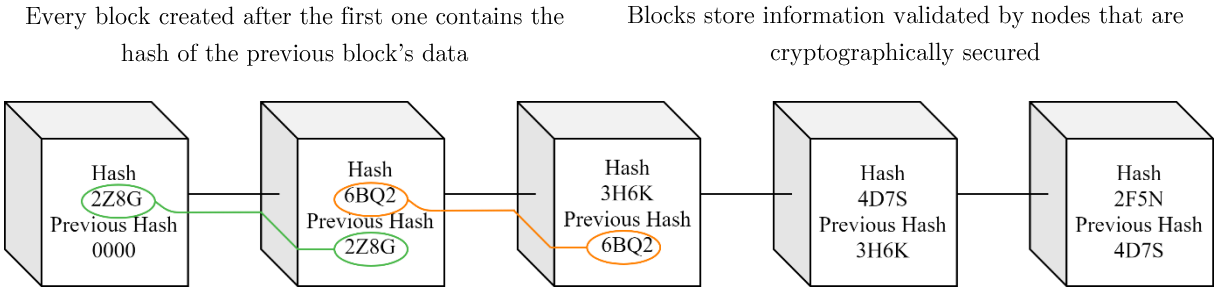


Figure 1-3 A blockchain design

1.8 Types of blockchain

The typical distinction made on the internet and many research papers is that there are public blockchains (or permissionless) and private blockchains (or permissioned). Both are decentralized peer-to-peer networks where each participant maintains a replica of a shared append-only ledger of digitally signed transactions. However, the level of decentralization is different, public blockchains are more decentralized in nature than private ones (18) (19).

There are three different types of blockchains, which will be explained, as follows:

- Public Blockchain
- Private Blockchain
    - Consortium blockchain

1.9 Public blockchain

A public blockchain or permissionless blockchain is completely open and anyone can join and participate in the network without the need for any approval. The network typically has an incentive mechanism based on game theory that encourages more participants to join the network. Participants, called nodes, act as miners/validators[7] support the network, and create/validate the new blocks. Therefore, in a public blockchain:

- Anyone can download the code and manage a public node in their local machine, validate transactions in the network, and participate in the consensus process.

[7] Depending on the blockchain type, we can have a miner that is a node or part of a node in a Proof of Work consensus algorithm or a validator (also a node) if it has other type of consensus algorithm as Proof of Stake.

The above, allows anyone to participate in the process of which blocks are introduced in the chain.

- Anyone can make transactions in the chain. Any valid transaction will be added.
- The transactions on the blockchain are public, which means that using a block explorer it is possible to see the information contained in the blocks. Any user can see any transaction made in the blockchain. Even when the information contained in the blocks is public access, these are anonymous as they are not associated with the identity of a specific person, but rather an anonymous address.

In the public blockchain of Bitcoin, the largest to date, running a public node means downloading around 150GB of information and about 2GB of RAM is required. Of course, not all the nodes have that size, over the years, different blockchains have been emerging as alternatives to the blockchain of Bitcoin requiring less memory to run a node.

1.10 Private blockchain

All the permissions for the blockchain are kept centralized. Usually designed for a single company that wants to share data with specific actors but does not want their sensitive data to be public. In a private blockchain, miners or validators are not needed. This is because all nodes in the private network are known and trusted. The number of nodes who validate the blockchain and the number of them adding the blocks are fully controlled and transactions are available only for the participants of the network who approve participation of new nodes. Private blockchains can also restrict the activity of the participants, allowing only some of them to carry out transactions even if they are part of the network (20) (21). Examples: Hyperledger, R3 Corda.

Consortium Blockchain: it is a specific case of private blockchains. This type of blockchain is controlled by pre-selected nodes and are not considered fully decentralized by nature. The distinction with a private blockchain is that rather than be controlled by a single entity, there is a group of actors that control the blockchain.

It is important to note that since these blockchains, by maintaining a centralized and permissioned structure (participants must be authorized by a central entity or a group or a group of participants), strictly speaking, they do not offer many advantages over a centralized database in terms of security and decentralization, but they do for the inclusion of smart contracts (explained later in *Chapter 1.15*), the use of consensus mechanism (in case of a consortium blockchain) the possible interoperability with other blockchains or the use of blockchains in a mixed way (certain data in a public blockchain and other in a private blockchain) could be an advantage compared to managing everything in a traditional database.

1.11 Permissionless and permissioned, a detailed approach

The previous classification is the usual one and the one we can find in most of the current literature. However, there are some researchers (22) that makes a distinction even between a private blockchain and a permissioned one, and between public and permissionless. So, the caveat is made that the classification of blockchain types is an issue that is still under discussion and development. In the case of an IoT network, it is convenient to make a distinction between both categories, thus creating a total of four categories

Depending on who has access to participate in the network, it can be differentiated between public and private blockchains. And depending on the authorization to add data to the blockchain or, in an IoT network, it can be differentiated between permissionless (no need of authorization) or permissioned. It is reiterated that this type of classification is quite new and represents a more detailed look at permits, which may be needed in the future given the inclusion of an IoT network. Since the limit of the definitions depends on whether people understand restrictive as any type of restriction (by immediately classifying the blockchain as private) or the restriction level depends on if it restricts the authentication or the authorization for permits. In *Table 1-4* a summary of the differences between each type of blockchain can be seen.

		Public Blockchain	**Private Blockchain**
Access Level (Authentication)		Anyone can join	Only authenticated nodes can join
Consensus mechanism		PoW PoS DPoS PBFT PoA	Multi-party consensus/voting
Performance		Low performance[8] Slow transaction speed	High Performance Fast transaction speed
	Permissionless	Participants can share/write data	Not authorized nodes will only acknowledge its existence, but not share any data (or have limited permission as only-read)

[8] By default, the higher the level of decentralization, the lower the performance. However, methods are being developed to increase efficiency and maintain decentralization. Sharding, 2nd layer solutions and new consensus mechanism are being developed and are explained in later sections.

Authorization	Permissioned	Pre-approved participants only can write/share data but everyone can read the data	Pre-approved participants only can write/share data

Table 1-4 Detailed approach of types of blockchains

This way of classifying blockchains may be more useful in the field of an IoT network, since, depending on the system architecture, it may be necessary to differentiate between the permissions to authorize the device and a different one to authenticate it. Next, in *Figure 1-4* certain projects are exposed that could be classified differently with this more detailed method.

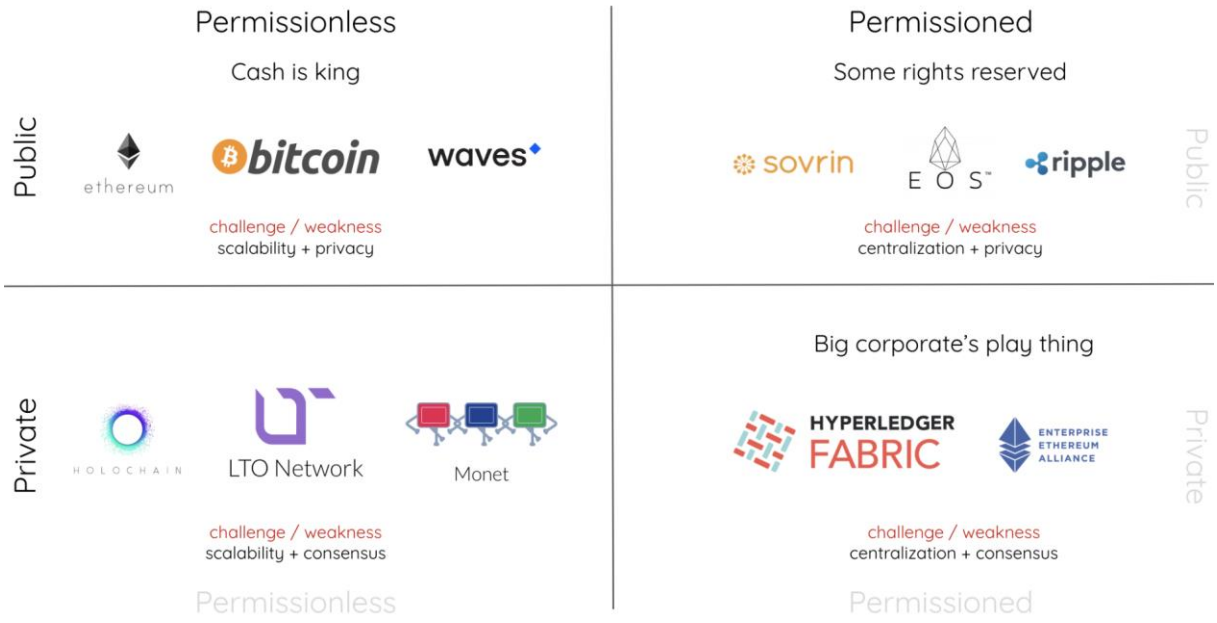


Figure 1-4 Different projects classified with the detailed approach

1.12 Decentralization

At this point, it is important to clarify the difference between a distributed and a decentralized system. Although the words seem similar, there is a fundamental difference in their meanings. By definition, all decentralized systems are distributed, however, not all distributed systems are decentralized. For example, in the case of a blockchain or a database, distributed means not all the processing of the transactions are done in the same place. However, a system is decentralized only when there is no central entity that controls these transactions or information flow. For example, if we think of a gas company, its sales points are distributed, however, the control of them is centralized.

Now, the benefits of a decentralized system will be explained. It is important to emphasize this issue since it represents the main difference between the different types

of blockchain mentioned. A public blockchain is the most decentralized, a consortium is partially centralized and a private blockchain tends to be centralized (23).

Now, the benefits of a decentralized blockchain will be mentioned (24):

- Fault tolerance: decentralized systems are less likely to fail accidentally because they rely on many separate components. Therefore, if well designed, one or more components that fail do not compromise the operation of the entire system.
- Attack resistance: A decentralized system is less likely to be attacked, due to the presence of many players. The economic effort necessary to attack a network composed of many actors is greater than that of attacking one or few.
- Collusion resistance: It is improbable that participants in a decentralized system to collude, at least to a lesser extent than in a centralized system. As is the case with people, collusion between a small group of people with power is much easier than many people with different incentives. This happens especially in a public blockchain, where in general the participants are anonymous.

The level of decentralization of the blockchain can be classified in different aspects, and a great classification of it is found in the words of the creator of Ethereum, Vitalik Buterin: *"Blockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state and the system behaves like a single computer)"* (24).

In summary, four main properties of blockchain technology which has helped it gain widespread acclaim are as follows:

- Decentralization
- Security
- Transparency
- Immutability

However, as shown later in *Chapter 4 blockchain challenges*, these characteristics are related to each other and often there is a trade-off between them.

1.13 Consensus algorithm

Investigators had been investigating since the 1980s how to reach an agreement between all entities in a distributed and decentralized system when some entities could be corrupted or controlled by an external agent. This problem, called Byzantine general problem[9] (25), does not exist in the vast majority of computer systems at present, since

[9] Byzantine general problem is a condition where actors must agree on a concerted strategy to avoid catastrophic system failure, but some of the actors are unreliable. In the scenario, a component of the network can

being central, decisions are carried out by a central entity and a common agreement is not needed. However, with the appearance of blockchains, this problem arose again. Participants in the network have to reach an agreement on whether a block is going to be included or not. The nodes must verify and decide together which blocks are added to the chain, and the decision mechanism called "consensus algorithm" varies from one blockchain to another. This consensus algorithm must be Byzantine Fault-Tolerant in order to avoid the Byzantine General Problem.

Below, a list from the first consensus mechanism invented to other alternatives that have emerged in recent years is shown.

Proof of Work (PoW): it is a probabilistic solution to the Byzantine Generals Problem (25), which means the confidence that a consensus is reached is growing with every block added to the chain, but it never reaches 100%. It is the first consensus mechanism and was introduced by the first blockchain ever existed: The Bitcoin's blockchain in order to avoid the Byzantine General Problem. To select a block, a cryptographic problem must be solved, where the probability of solving that problem depends on the computational power of the node. The higher computational power, the higher the odds to solve the problem. Since computational power is proportional to electricity consumption, the more the computational power, the more the difficulty of the cryptographic problem and therefore more energy cost to maintain the network.

Proof of Stake (PoS): it is a less energy-consuming algorithm. Those who own a higher amount of coins or tokens[10] are the ones that have invested the more in the network. To participate in the selection of the next block, nodes have to "stake" [11]a number of coins or tokens. In general, the higher the number of staked tokens, the higher the chances to become the block validator[12].

Delegated Proof of Stake (DPoS): for many, it is the evolution of the PoS and it closely resembles the democratic elections of the countries. It has the advantage that it consumes less energy than the PoW but also allows and encourages voters with fewer tokens to vote for the delegate who has better proposals. In a DPoS consensus system, users can stake their tokens to vote for delegates. A delegate is an entity that wants to produce a new block. Delegates with a higher number of votes are selected by the system to create the next block to be added to the chain.

---

inconsistently appear as failed and functioning to a failure-detection system, presenting different symptoms to different observers.

[10] Tokens are a representation of a particular asset or utility, that usually resides on top of another blockchain.

[11] Staked tokens are locked up tokens for a defined amount of time.

[12] Node who is allowed to produce the next block.

Practical Byzantine Fault Tolerance (pBFT): In the pBFT consensus, there is a primary node (leader) that receives the order from the client, and others that are considered secondary nodes and have a backup role. The role of the leader will be changed if necessary, each secondary node can become a leader (usually when the leader fails). There is an assumption that malicious nodes in the network cannot simultaneously equal or exceed $\frac{1}{3}$ of the overall number of nodes in the system. Honest nodes help in reaching a consensus regarding the state of the system using a majority rule. The pBFT consensus model works efficiently only when the number of nodes is small due to the high communication overhead that increases exponentially with every extra node in the network. For example, Harish Sukhwani et al. conduct a successful simulation, using Hyperledger Fabric with a total of up to 100 peers (26). Therefore, this method is well-suited for private blockchains (e.g. an Hyperledger project) that are controlled by a third-party (27).

The consensus algorithm or mechanism is an important variable to consider since, as will be explained later, it affects the performance of the network, as well as its scalability. A more detailed analysis of which are more suitable for use with IoT devices will be discussed in *Chapter 4 Blockchain challenges.* In addition, the choice of one or the other also determines how decisions will be made that will affect the blockchain and its possible future changes (soft forks or hard forks).

1.14 Soft fork versus hard fork

Basically both present changes in the blockchain network, for example, if the network needs to increase its scalability at some point, or an error has been found in the base code and a security update must be performed, a soft fork or hard fork will be necessary depending on how drastic the code change is.

To define hard fork and soft fork, first, two more basic definitions will be introduced.

Fork: "A fork is a moment you have a protocol version which is different from the main one." (28). It is an open-source code modification. If not all the nodes replicate the same data, a fork can happen accidentally, but usually accidental forks are detected and resolved. In short, a fork is a change that updates or changes the previous code. As will be seen below, it can be classified as a hard fork or soft fork.

Hardfork: it renders the older version of the blockchain invalid. Changes as the block size, the difficulty of the cryptographic puzzle, or others require a hard fork. If older nodes reject the new protocol, the chain is split in two, therefore one running with the new protocol and other keeping the old one.

Softfork: A soft fork is a change in the protocol that still works with older versions. There is no need to split the chain if old nodes accept new blocks coming with the new protocol.

Blockchain protocol: "The blockchain protocol is the code convention which defines the connection, mining and transaction rules. To be a part of the network, you must comply with the protocol" (28). In the protocol find the rules that nodes must follow. For example, in the Bitcoin PoW protocol information as the size of the block, the rewards due to the mining activity, the block time generation, and many more can be found.

It should be mentioned that as new challenges or situations occur over time, it is important that the network protocol is kept up to date. Concrete cases of why a protocol would need to be updated:

- Fix a security risk found
- To add a new functionality

1.15 Smarts contracts

In order to understand the extent of IoT integration with blockchain, the smart contract needs to be introduced.

In the real world, a contract is an agreement between two parties. Generally used in the purchase and sale of services, projects or objects such as real estate or vehicles. A smart contract is a contract written into lines of code intended to facilitate, verify or enforce the performance of a contract. They are self-executing contracts with the terms of the agreement between buyer and seller that are executed on a decentralized infrastructure, therefore they allow trusted transactions without the need of a central authority.

The potential of smart contracts is very broad; however, its correct operation lies in the aforementioned characteristics of the blockchain (security, immutability, decentralization). For example, a smart contract could be created for the purchase and sale of a property. The agreement between the seller and the buyer would be stipulated in the smart contract, as well as the time and method of payment. With the information of the contract stored in the blockchain, the registration of the property as well as the identities of the users, the parties would only have to verify their identity through some IoT device (fingerprint, facial recognition, digital ID, etc.), the willingness to make the agreement and the monetary transaction in the blockchain. In a case like the previous one (assuming that the government accepted blockchain technology as a trusted intermediary), once the payment is made, the property registration would be automatically transferred by the seller to the buyer, without the need for any notary

to act as minister of faith. Cases such as the previous one, or voting in the elections through blockchain, are just some of the potential real use cases presented by the integration of the blockchain with IoT devices.

Many of the benefits and strengths of the blockchain have already been mentioned. The following section will discuss the challenges that must be resolved to be a competitive alternative to current information technologies. The challenges correspond to the blockchain in general, as well as those related to its implementation with IoT and smarts contracts, which play a leading role in the execution of automated transactions.

1.16 Smart contracts challenges

It has been mentioned that one of the benefits of smart contracts is the automatic execution that they can perform when a certain parameter that triggers the contract is fulfilled. However, there are many cases where, although it sounds quite easy in theory, in reality, the execution of the contract is impossible. For example, the market for agricultural insurance policies could benefit from the use of smart contracts. Among some of its products, a potential insurance service that responds in case of unusual droughts or low levels of rainwater could be created. Using IoT devices, the data collected by them would inform the insurance company if the levels of rainwater were below the established limits and thus automatically activate the insurance policy.

However, there is a big problem that interferes before the execution of the smart contract by themselves. Since the blockchain is based on a consensus mechanism where all participants must agree on the information, each node should execute the smart contract and obtain the same data to agree. In this way, the decentralization of information would be maintained. Then, given some delay between the time that the IoT device sends the information to each node, the weather information could change slightly causing the nodes to not reach a consensus.

To solve the above, it is necessary to include another actor in the network that will be explained later in detail: the oracles. Oracles are one or more trusted parties that enter data to the blockchain from the real world. So, once the information is entered into the blockchain, the nodes could analyze the information and reach a consensus (since the information seen by the nodes will be the same for everyone). Below, Figure 1-5 represents the theoretical operation of a blockchain in operation with information oracles. The nodes (represented as gray cubes) oversee that the information entered has integrity with the information already registered in the blockchain (white cubes). However, they cannot fully verify that the information entered by the oracle is correct. For example, if the oracle is in charge of entering the information of the dollar value,

the nodes verify that the information entered corresponds to that previously registered oracle (and not another one) and that the information corresponds to the dollar type. However, they cannot verify that the price of the dollar is correct, which could happen in the event that the oracle, or source of information, is manipulated.

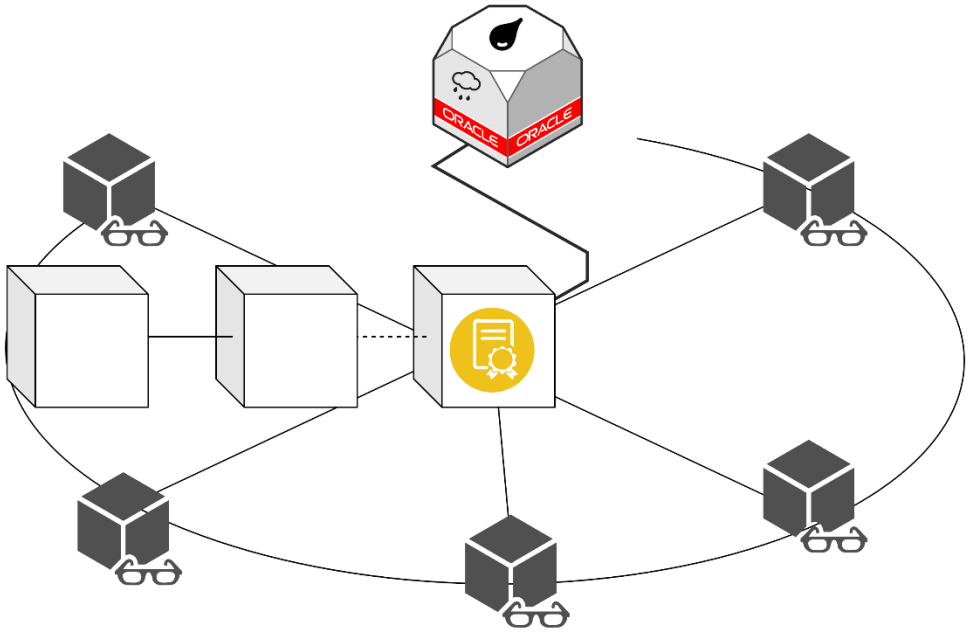


Figure 1-5 Representation of a blockchain connected with an oracle

The flow of information as follows: an oracle pushes the information to the blockchain rather than a smart contract that requests it from the outside world. However, there is another problem that arises with the use of oracles and that is that by trusting in a trusted part, one falls back into a centralized model that loses the benefits of decentralization. The question is then, how we make sure that the information that will enter the blockchain is also decentralized and therefore, reduce the risk of manipulation and increase the reliability of the information source. Given the above, a case study will be explained later in *Chapter 6* where it is detailed how that problem is potentially solved.

2 Internet of Things

This section will introduce the Internet of Things universe (IoT), its current use, and its potential. It will also expose the exponential growth it has had in recent years and its growth projection.

Internet of things is a phenomenon proposed in 1999, by Kevin Ashton, in the Auto-ID Center at MIT (3) and it refers to the digital interconnection of everyday objects with the internet. It is, in short, the internet connection more with objects than with people. The Internet of things powers objects that were formerly connected by a closed

circuit, such as communicators, cameras, sensors, and so on, and allows them to communicate globally through the use of the network of networks. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), microservices, and the internet. Convergence has helped tear down the data silo between operational technology (OT) and information technology (IT), allowing unstructured data generated by machines to be analyzed for information that drives improvements. In an IoT ecosystem, most of the communication is in the form of Machine-to-Machine (M2M), so no human interaction is involved in common processes (29).

The exponential diffusion of the Internet of Things applications in different areas such as cities, companies, even people's homes, and cars is being experienced. The adoption of IoT devices is generating a great impact both in daily lives and in different sectors of the industry including transport, cities, the supply chain, energy management, manufacturing, and many others. But with an increasing number of IoT systems, the security, availability, and reliability of the system are some of the critical aspects to ensure the progressive growth of the network (30). Next, certain aspects present in an IoT network that needs to be known to understand the operation of an IoT network will be defined.

Interface: it provides a visible structure that can be easily utilized by the user. The interface needs to be user-friendly so it will be easily understood by a non-developer person.
Devices: single units that can be sensors (responsible to collect and transduce required data), actuators[13], routers[14], among other IoT devices in charge of data gathering and control.
Computing: it is the real-time availability of computer services. For example, the cloud storage service or cloud computing power, Fog computing using a local processing unit, etc.
Gateway: it can be either a physical device or software. It is a bridge between the cloud and the devices. It performs the data transformation from the devices to the cloud environment, enabling easy management of data traffic between protocols and networks (e.g. the cloud).
Protocol: it is the system of rules that a device follows. It is important to have compatible protocols between devices so that the ecosystem is efficient.
Client: a client is the receiving end of a service or the requestor of service in a client/server model type of system.

[13] An actuator is a component of machines that is responsible for moving or controlling a mechanism or system. It works on the basis of the decision taking by the computing node.
[14] It is a hardware product that allows you to interconnect computers that work within a network. Its function is to be responsible of establishing the route that will be allocated to each data packet within a computer network.

2.1 Internet of Things architecture

First, the internet layer will be explained in a very general way. Since the beginning of the Internet, the protocol in charge of directing information has been called IP. An IP address is a number that logically and hierarchically identifies an interface of a device (usually a computer) within a network that uses the Internet protocol. The most used IP protocol in the last decades (since 1983) has been IPv4, however, the protocol has a problem that limits its expansion, and it is the limited number of 4,294,967,296 or 2^{32} unique addresses given its architecture of 32 bits. That is why, for a world in which there are already billions of devices connected to the internet and with a continuous growth in demand for IPs, a new version of the protocol was necessary, this being the so-called IPv6 protocol. In contrast to IPv4, the IPv6 system is based on 128-bit addresses and can facilitate close to 340 undecillion or 2^{128} unique IP identifiers. This is a massive increase in capability that would be sufficient for the exponential growth of IoT devices for the next decades.

Besides the internet, many elements are involved in an IoT network. Among them, the following can be mentioned as sensors, protocols, actuators, cloud services, and layers. These elements can be found in different and essential stages in the architecture of an IoT network. The main components of an IoT architecture are (represented by *Figure 2-1*):

1. Sensors and actuators
2. Internet gateways and Data acquisition systems
3. Edge IT
4. Data center and cloud

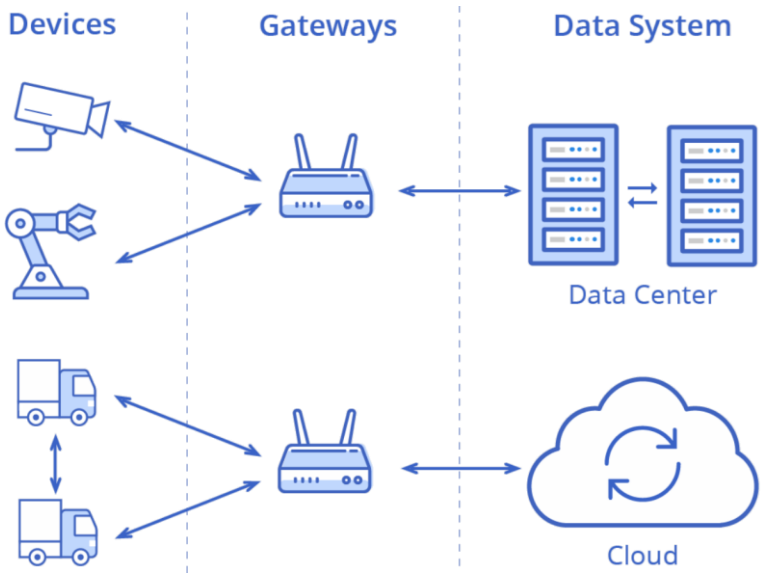


Figure 2-1 Basic IoT architecture by components based on cloud computing

In an IoT ecosystem, there is no single consensus or single architectural design that is out there which is agreed universally because each company each organization, and

each user have different requirements depending on the matter. A simple three-level architecture could be:

- IoT device layer – perception layer
- IoT gateway layer – network layer
- IoT platform layer – application layer

In *Figure 2-2*, the function of each of the layers is simply summarized.

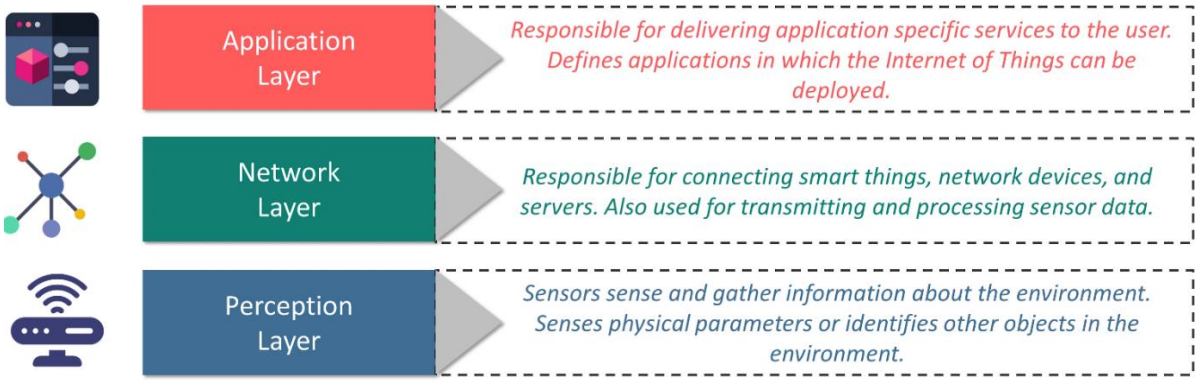


Figure 2-2 IoT architecture by layers

In *Figure 2-3,* a breakdown of the IoT architecture both by layers and by components is shown, where some specific examples of applications, gateways, and devices are also included.

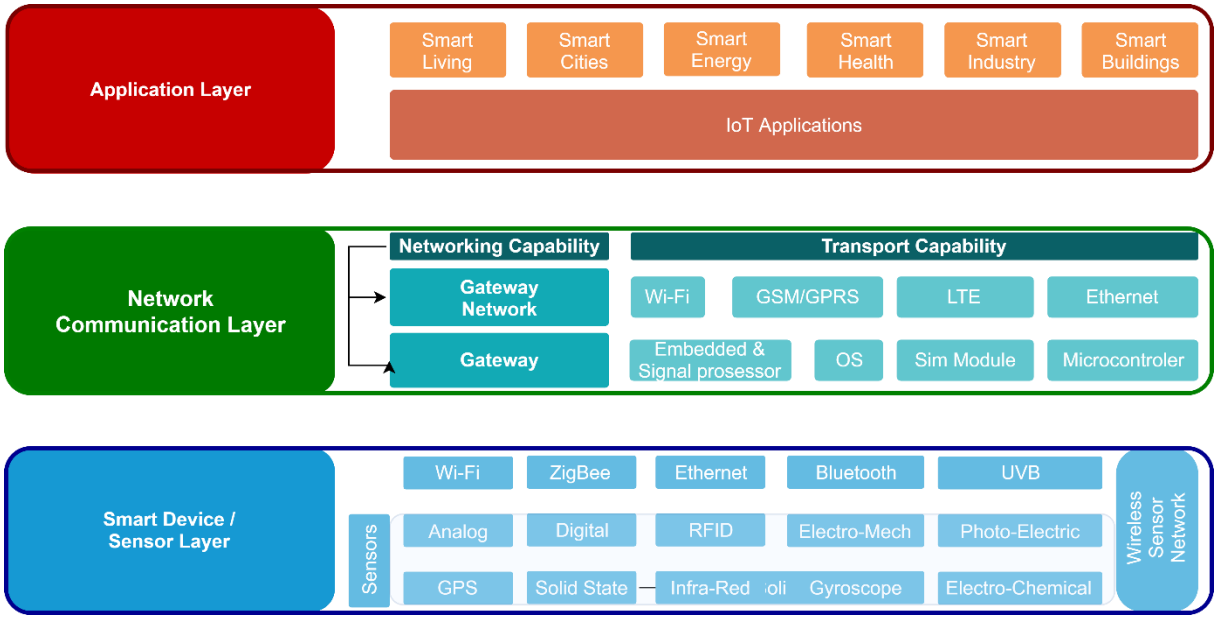


Figure 2-3 IoT architecture breakdown by layers and components (31)

2.2 Types of IoT architectures & standards

Cloud-based architecture: it is a worldwide network of servers that work together as a single ecosystem that manages stores and processes information, this in order to allow the operation of services that users access through the internet such as social networks email, streaming of movies, and series, etc. Cloud computing frees the

enterprise and the end-user from the specification of many details (31). It is an architecture that enables ubiquitous and convenient shared access to a pool of configurable resources (32). This architecture was well working until the appearance of latency-sensitive applications, which usually require the data source close to them to meet delay requirements.

Fog Computing architecture: in fog computing architecture, unlike cloud computing, data instead of being sent to very distant servers is processed near the device and does not require an internet connection to work. Fog computing is the processing, administration, and storage of information but through the internet of things devices. Instead of connecting to a remote server online, IoT devices interact with each other in a local area network (LAN) without the need to send the information to the cloud or the internet. In turn, this information can meet the cloud in cases where necessary. For the moment, in fog computing models, some of the critical operations that used to be processed by cloud servers are now assigned to be performed by IoT hubs or fog (33) (31).

> Advantages: no internet connection required, easing the load on internet bandwidth (data transmission capacity). Only the necessary information is sent in summary form to the data centers. Response times are shorter since it is performed locally.
>
> Disadvantages: since the information is being treated on devices within the physical reach of anyone, it is susceptible to physical alteration attacks to violate the security of the devices. The attack or exploitation of the vulnerability of a device would compromise the security of the rest of the devices connected to fog computing given the existing data interconnection.

Edge Computing standard: it seeks to improve latency and save bandwidth, optimizing the system bringing computation power, intelligence (as artificial intelligence or machine learning), and data storage closer to the source of data (e.g. IoT devices). Thus, processing capabilities and intelligence (as artificial intelligence or machine learning) closer to the IoT devices. Edge computing reduces the need for long travels for the data, reducing the distance between the source and the server. Currently, data is increasingly being produced at the edge of the network, cloud computing is not efficient for data processing of this kind (34). Compared to Fog computing, Fog is the standard, and Edge is the concept, so they are very related (35).

In *Figure 2-4*, the architectures mentioned above are represented.

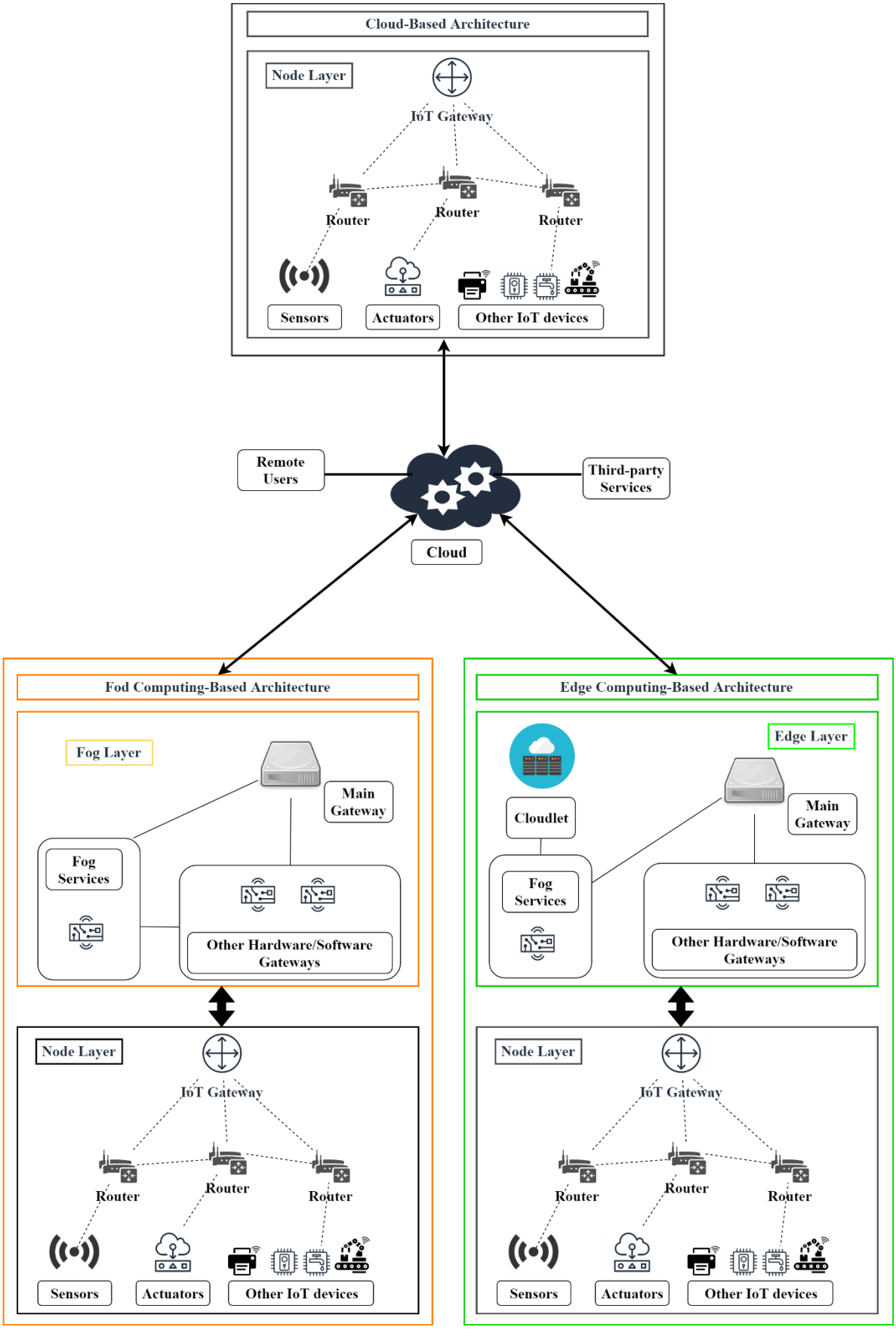


Figure 2-4 IoT-based architectures (18)

As can be seen in *Figure 2-4*, The Fog, and the Edge computing layer with very similar, and that is as already mentioned, its objective is very similar. The difference is that the Fog computing layer is concerned with interconnecting IoT devices in a LAN network, while Edge computing also brings the cloud system locally (in the figure identified as cloudlet[15]), where it can have a local cloud of storage, processing power, or another needed feature. Both are still connected to the cloud, but this is only used to perform specific tasks, thus reducing the need for use and improving response time and bandwidth.

2.3 IoT applications

The Internet of Things is changing the way the devices relate to each other. Among the applications of the IoT, examples from different sectors such as industrial, domestic, and smart cities that facilitate many of the day-to-day tasks can be found. IoT is becoming a reality and is gradually being introduced into our lives. Gathering and connecting data points from physical objects is the key to letting new IoT business cases come to life. In *Figure 2-5*, some of the IoT applications are presented.

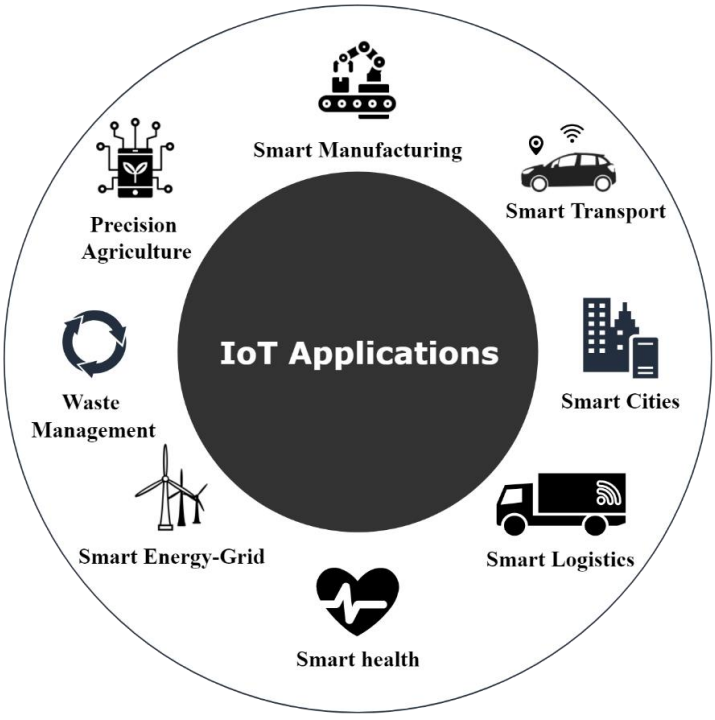


Figure 2-5 Some IoT applications

The following paragraphs briefly describe some current use cases in which the industry is integrating with IoT devices.

[15] A cloudlet is a mobility-enhanced small-scale cloud datacenter that is located at the edge of the Internet. The main purpose of the cloudlet is supporting resource-intensive and interactive mobile applications by providing powerful computing resources to mobile devices with lower latency.

Precision agriculture
Smart farms are a fact, the quality of the soils is decisive to produce good crops, and the Internet of Things offers farmers the possibility of accessing detailed knowledge of their conditions. By implementing IoT sensors, a significant amount of data can be obtained on the state and stages of the soils. Information such as soil moisture, acidity level, the presence of certain nutrients, temperature, and many other chemical characteristics, helps farmers control irrigation, make water use more efficient, specify the best times to start planting, and even discover the presence of diseases in plants and soil.

Intelligent power distribution
The progressive use of smart energy meters, or meters equipped with sensors, and the installation of sensors at different strategic points ranging from production plants to different distribution points, allows for better monitoring and control of the electricity grid. By establishing a two-way communication between the service provider and the end-user, information of great value can be obtained for fault detection, decision making and repair.

Smart health
Physical activity monitors are a hot topic in workplace health programs, but similar data can be used to help educate health care providers and insurance companies as well. The use of wearables, sensors connected to the beds of the patients or directly to them, allows doctors to monitor their conditions, outside the hospital and in real-time. By receiving metrics and automatic alerts about the person's vital signs, the Internet of Things ecosystem helps to enhance care control and the prevention of lethal events in high-risk patients.

Smart transport
The Internet of things can be very useful in the management of vehicular traffic in large cities, contributing to the concept of smart cities. When mobile phones are used as sensors, collecting and share data from the vehicles through applications such as Waze or Google Maps, the Internet of Things is being used to inform people and at the same time contribute to traffic monitoring, showing the conditions of the different routes, and feeding and improving the information on the different routes to the same destination, distance, estimated time of arrival. In the future, with the arrival of cars with autonomous driving, vehicles will be able to communicate with each other, drastically minimizing traffic jams and crashes as they would move in a synchronized fashion.

Smart city

A smart city can be defined as a city with a well-performing forward-looking way in economy, people, governance, mobility, environment, and living, built on the smart combination of endowments and activities of self-decisive, independent, and aware citizens. The application of digital technologies of smart cities can be in general divided into three categories Internet of things, e-governance, and e-democracy. As will be seen later with the consensus mechanisms, e-democracy and e-governance can be carried out using blockchain technology. There are four aspects that are included in smart cities as mentioned by Elmangoush et al. (36):

- Smart infrastructure provides an interconnection between Humans and machines (H2M) and between machines (M2M).
- Smart operations: to provide and support operations and management of the city. Integrating systems and information that allow providing innovative services to citizens and companies.
- Smart ecosystem: which would be analyzing the collected data to enhance the system performance, improve process outcomes of it as well as for organizations and companies value chain.
- Smart governance: to increase the usability and quality of services and products, the developers need to work together with the different actors in the city, discussing ideas, experiences, and knowledge in general.

As the number of connected devices embedded in cities' critical infrastructure increases, an attack on the infrastructure of the network supporting these devices could be critical in the smart city functioning. It is also important to highlight the importance of protecting the private data of the citizens such as medical records or bank statements collected by the E-Governance which could be compromised by corruption or other sources of manipulation.

2.4 IoT devices constraints & challenges

As can be seen in the previous *Figure 2-3*, IoT devices include both resource-constrained and resource-rich devices. For example, a Raspberry Pi[16] device, together with certain sensors that allow it to act as an IoT device, can support enough resources to store a large amount of data or carry a large battery. However, there are also IoT devices with very limited resources such as energy, processing power, memory, among others (37). Therefore IoT devices and protocols must be designed to be efficient in the use of resources to keep real-time processing, but also to maintain good connectivity, protect privacy and provide a secure network (38). In *Chapter 3*, the restrictions associated with the use of blockchain technology will also be discussed in detail. In the case of IoT applications, they still suffer from two major issues: high costs and insufficient security. The building and maintenance process of large-scale centralized

[16] The Raspberry Pi is a series of small single board to promote teaching of basic computer science in schools and in developing countries.

cloud platforms may involve high amounts of operational expenditure to connect all devices. Another inconvenient is the lack of compatibility between the different providers of the cloud services (or other IoT related services), the above involves a high cost to implement an information exchange hub working across different cloud providers (39). Some IoT applications might require very short response time, some might involve private data, and some might produce a large quantity of data which could be a heavy load for the network (22). Among the fundamental features that an IoT network should provide and the challenges it faces, it can found (40) (4) (36):

- Scalability: the number of IoT devices that are going to be managed is going to be at least one order of magnitude bigger than the number of currently connected devices to the internet. Therefore, the capacity of the network to grow is a fundamental characteristic.
- Identity management: even if trillions of IoT devices are going to be connected to the internet over the next years, each of them must be identifiable by a unique Id to provide an efficient and automatized management of the devices (this was one of the reasons why the IPv6 protocol had to be created).
- Interoperability and interconnectivity: anything should be able to be connected to the global information and communication structure. The standardization of IoT is important to provide better interoperability for all the devices.
- Security: related to personal data and physical well-being. Security must be along with the network, starting and endpoints to prevent unauthorized access. The larger the information handled by the system, the greater its security should be.
- Digital Governance: in some cases, as Smart Cities, to manage the overall system consistently, discussion and decision making must be taken with a horizontal approach. However, finding a form of digital participation in decision making is the main challenge.
- Privacy: the architecture needs to be technologically capable of preserve privacy when the data requires it and also be able to determine who can see the data and who cannot.

2.5 Market integration and prospective

It is known that the market for IoT devices is increasing. Today a data-driven world is being experienced, which is changing faster than ever before and now some new actors add up, IoT devices. The integration of IoT devices in people's daily lives is a reality that is increasing. Smart TVs, wearable devices, home automation, many are the examples of IoT devices with which people interact on a day-to-day basis. On the other hand, the use of sensors and automated machines that take advantage of the benefits of IoT, are increasingly used in the Industry. IoT devices are here to stay and their growth is projected exponentially.

Market studies such as the one carried out by the market consultant firm Grand View Research value the IoT market size at USD 161.14 billion in 2018 and USD 949.42 billion by 2025 (41). Others have forecast a compound annual growth rate (CAGR) of 12.6% during the period 2017-2022 and a worldwide technology spending on the Internet of Things of $1.2T in 2022 (42). As exposed, depending on the study and its methodology used, the estimates vary. The truth is that although the forecasts vary, they all agree that the market will grow exponentially. Below, *Figure 2-6* (43), shows the overall market expenditure in IoT.

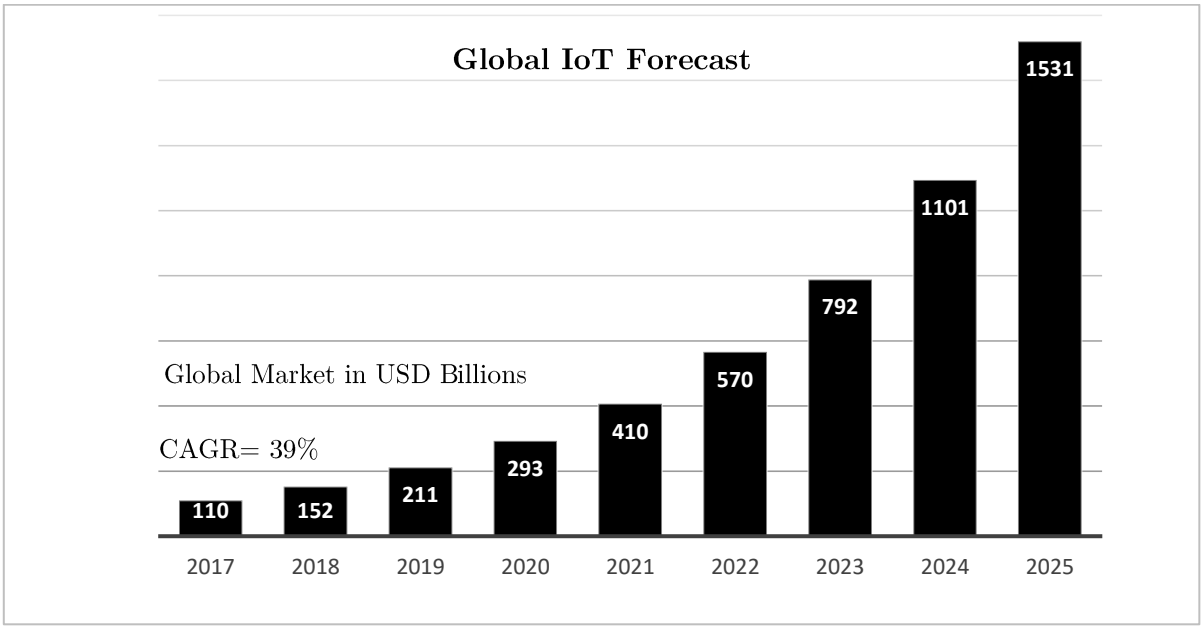


Figure 2-6 Global market IoT forecast IoT analytics research 2018 (43)

As for the number of connected devices, there are estimations between 20 and 25 billion things to be connected to the Internet by 2020 (44) (45). According to the study carried out by the DBS bank group, IoT would be reaching the inflection point of 18-20% in 2019, from which growth will start to accelerate, being one of the fastest growing segments in the technology industry (46). Following the theory set forth by Everett Rogers, which seeks to estimate the rate of adoption and diffusion of innovative ideas (47) and regarding the adoption of IoT devices, it is still in the early stage, moving from the section of early adopters to early majority. It is possible to see the curve of adoption in *Figure 2-7.*

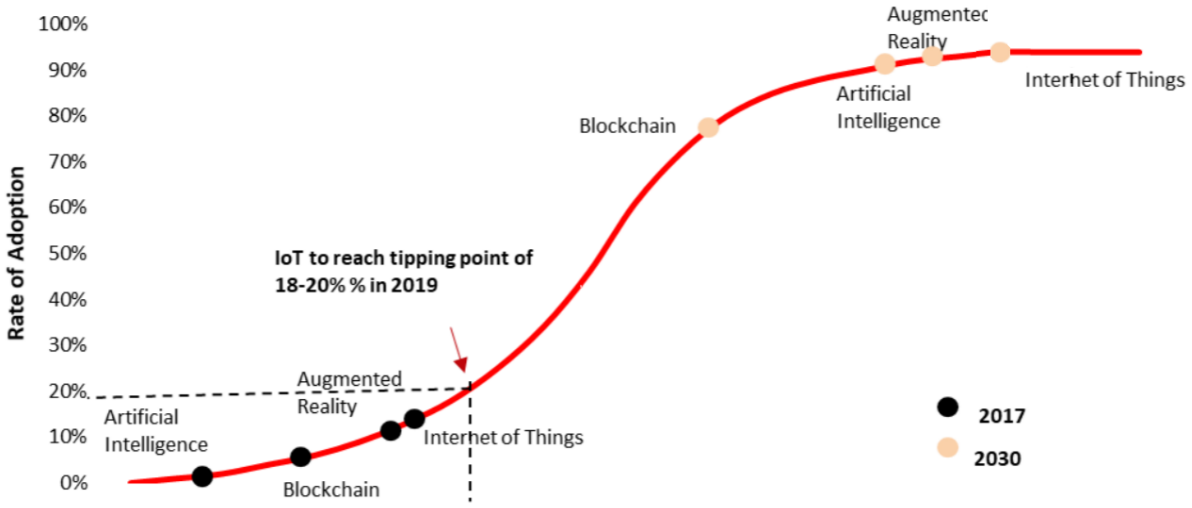


Figure 2-7 IoT adoption over the next 10 years (46)

As for the industry, the proportion of companies using IoT (adopters) has more than doubled in the last years. Adoption has risen from 12% in 2013 to 29% in 2017. Transport and logistics (19% to 27%) and retail (20% to 26%) have shown the largest year-on-year gains from 2016. Most of the organizational adopters are implementing IoT to increase efficiency in their business, manage risk and reduce costs (14). From these data, it can be seen that although the industry is rapidly adopting IoT technology, they are still far from reaching the percentage of adoption in people estimated at 63% of the total IoT devices (46). As will be seen in the next *section 2.6*, there are still challenges facing the industry in order to exploit the potential of IoT, where data security is one of them.

Parameter	2016	2017	2018	2019
IoT units installed base – total (m)	6,382	8,381	11,197	125,000
Consumer devices (m)	3,963	5,244	7,036	75,000
Consumer devices as % of total devices	62%	63%	63%	60%
Connected devices per person	5	5	5	5
World population (m)	7,400	7,600	7,700	8,500
IoT adoption rate	11%	14%	18%	176%

Table 2-1 IoT estimations (46) [17]

2.6 Industry perspective

In this section, a brief analysis of the adoption of the industry and IoT devices is carried out, regarding the results of the companies that have already adopted the technology and the current reasons that stop adoption in the industry. Below are some points about companies that have already included an IoT ecosystem in their processes. The

[17] Estimations based on estimates by Gartner, United Nations, World Bank (46).

data is mostly collected from a study carried out by the Vodafone group, in conjunction with Circle Research (14). In a universe of 1278 companies, the results related to the IoT universe obtained were as follows:

- Among the IoT adopters, 95% achieved tangible benefits, while those with a higher number of connected devices are achieving the biggest gains.
- More than half of the companies are increasing their revenue or creating a new revenue stream. Among them, the average increase in revenue after IoT adoption averaged 19%, more while the reduction in costs was 16%.
- According to respondents, 88% of them are investing more money in the adoption of IoT devices than 12 months ago.

The study carried out by (14), has been carried out continuously since 2013 and involves both small and large companies. Since that year where adoption was around 12%, it has been growing to reach 29% in 2018. From the state of the industry market by sector, the highest percentage of adoption and growth in the sector of energy and utilities. Next, the percentage of adoption according to the number of devices used by the company is shown in *Figure* 2-8.

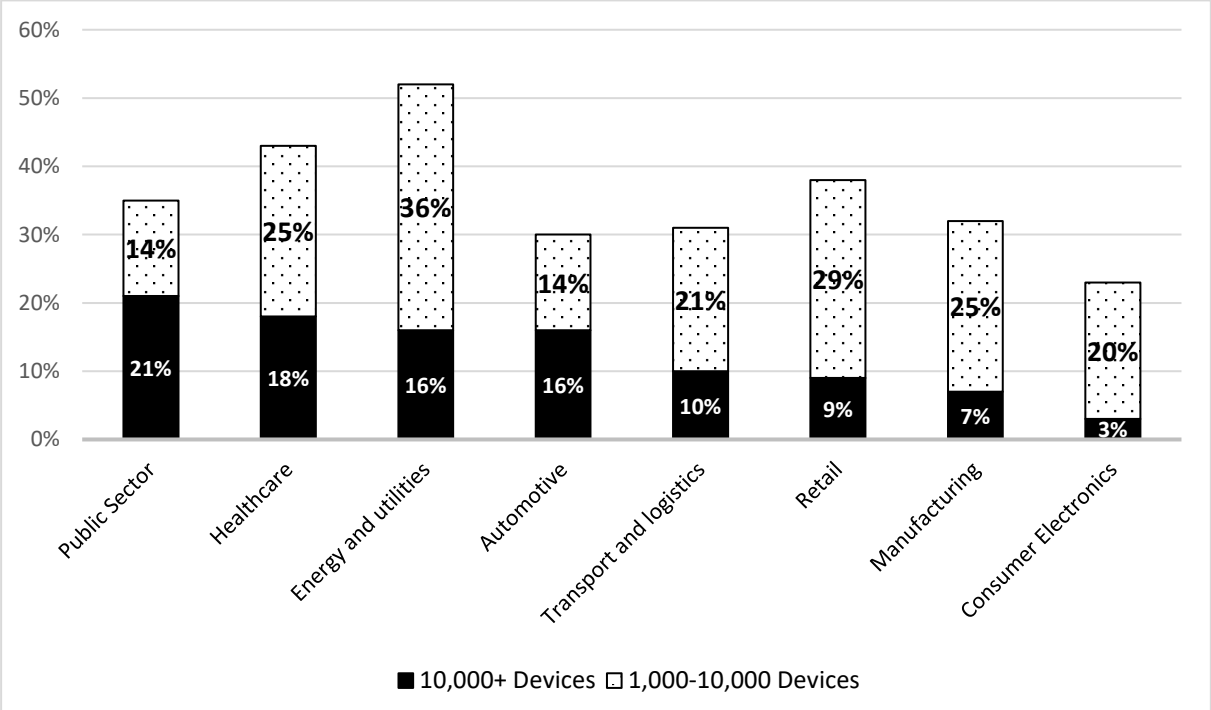


Figure 2-8 Percentage of adoption by the number of devices (14)

Among the uses that technology is given in this sector remote monitoring of services to customers can be found. That way, the company's specialized team does not need to constantly check customer consumption. It also improves the accuracy of overconsumption or the application of differentiated rates depending on the consumption schedule.

In the healthcare sector, some hospitals and clinics receive data from patients who are about to arrive when they are in the ambulance. In that way, the patient's condition is tracked and transmitted to the staff in charge of attending the emergency, who earn precious minutes by having the equipment ready before the arrival of the patient.

Examples like these can be found in each sector and are concrete examples of how IoT devices are changing the industry. However, as companies embed the automation and control of their processes through IoT devices, they face some critical decisions that they must face and resolve to continue with the development. Much of the information that is transmitted or captured by IoT devices are usually confidential or of utmost importance to the company, so maintaining a secure system is a priority. As companies create more complex systems that move more and more data, the greater the risk and cost of an incident or infrastructure attack. Therefore, it is not surprising that according to the Vodafone Group research, security and data report privacy concerns are still seen as the biggest barriers to IoT to further adoption (14). When handling a large amount of data, the system that is responsible for its management must be robust and secure, so the growth of the IoT ecosystem must go hand in hand with security.

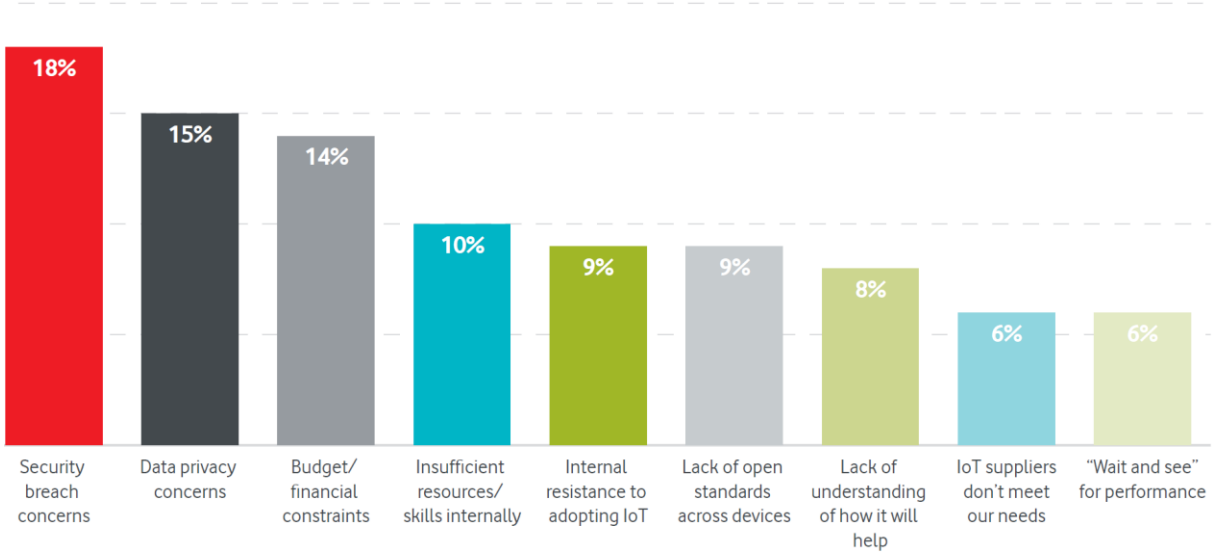


Figure 2-9 Concerns and barriers to adopt IoT of organizations (14)

As explained in *section 2.4,* the challenges of security and privacy that researchers expose (38) (36) (4) (40), is also perceived as a concern and barrier for companies. These problems can be addressed by blockchain technology, as well as contribute with other improvements to generate a secure, scalable, and robust IoT ecosystem and will be addressed in the next chapter.

3 Blockchain of things

The revolution of the Internet of things is building the way of a world where everyday objects will be interconnected interacting with the environment, collecting information, and automating tasks. To achieve the described vision, it is necessary to have an environment with data privacy, seamless authentication, security, robustness against attacks, easy deployment, and self-maintenance. These characteristics can be found in an open-source distributed ledger like the blockchain, which could enhance in many ways an IoT network and eliminate the need to handle communications from a central location. Blockchain technology can contribute in many ways to an IoT system, such as security, robustness, protection of privacy (if necessary), among other aspects. However, the current problem lies in the fact that the first blockchains designed do not have an architecture designed to complement an IoT system (22).

Currently, IoT devices lack the authentication standards and encryption necessary to keep user data safe. For example, in a traditional IoT architecture, there are security risks in identity registration and authentication processes. Current systems of IoT devices rely on DNS[18] registries of the IP addresses. These registries may be backed up by edge computing but being part and depending on a centralized system risks single points of failure [19] at the system (48). As it is known, blockchain has a peer-to-peer architecture, which gives its distributed nature. This architecture, allows devices to directly interact with each other to identify, authenticate, and exchange information without the need of any centralized node or agent between them (49). This means that the blockchain itself, not being controlled by a central entity, is not exposed to a single point of failure (11).

For example for an improved identity registration and authentication case, it can be assumed a case where blockchain provides an immutable record of all sensors and devices, the ownership of data, and all transactions on the other hand, with the use of smart contracts it's possible to automate the actions and processes. A similar case is proposed later, that proposes a blockchain-based software authentication system. Connect IoT devices in a decentralized manner could benefit greatly the network through the verification of truth and transactional agreements that encourage devices to share their properties and data in real-time. This gives birth to entirely new general-purpose applications and value chains.

As will be discussed later, In the future, there is the risk of suffer critical damage if hackers gain access to IoT devices. Standardization and authentication of IoT devices

[18] The domain name system (DNS) is a decentralized hierarchical nomenclature system for devices connected to IP networks such as the Internet or a private network. This system associates varied information with the domain name assigned to each of the participants.

[19] A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working.

should be integral to ensure widespread adoption of them. To overcome the security, privacy, and trust challenges, the IoT can leverage on the blockchain technology due to its decentralized architecture. If a blockchain-based network that connects the IoT devices can be created, both with which people interact day by day and those required in different industries (health, safety, manufacturing, traceability, property registers, etc.) the benefits of a verifiable, secure network with a permanent method of records that will allow autonomous decision-making can be exploited.

In *Chapter 1*, the general benefits of technology have been explained, as well as in the IoT chapter, many use cases are mentioned where an IoT system could improve the industry. This current chapter mentions use cases where IoT systems, in conjunction with blockchain technology, can be applied to improve current market sectors as well as create new market possibilities.

The blockchain technology as a whole of the IoT networks will be a fundamental part of the productive ecosystems of the future. For example, in the manufacturing sector, it is known that manual processes, carried out by human beings, are subject to much greater variability and errors than those executed by automated machines. An IoT blockchain network is going to be the next step of manual processes in the digital era, that in conjunction with other emerging technologies such as artificial intelligence and augmented reality, will allow an optimization of the processes in all the imaginable aspects safely and reliably.

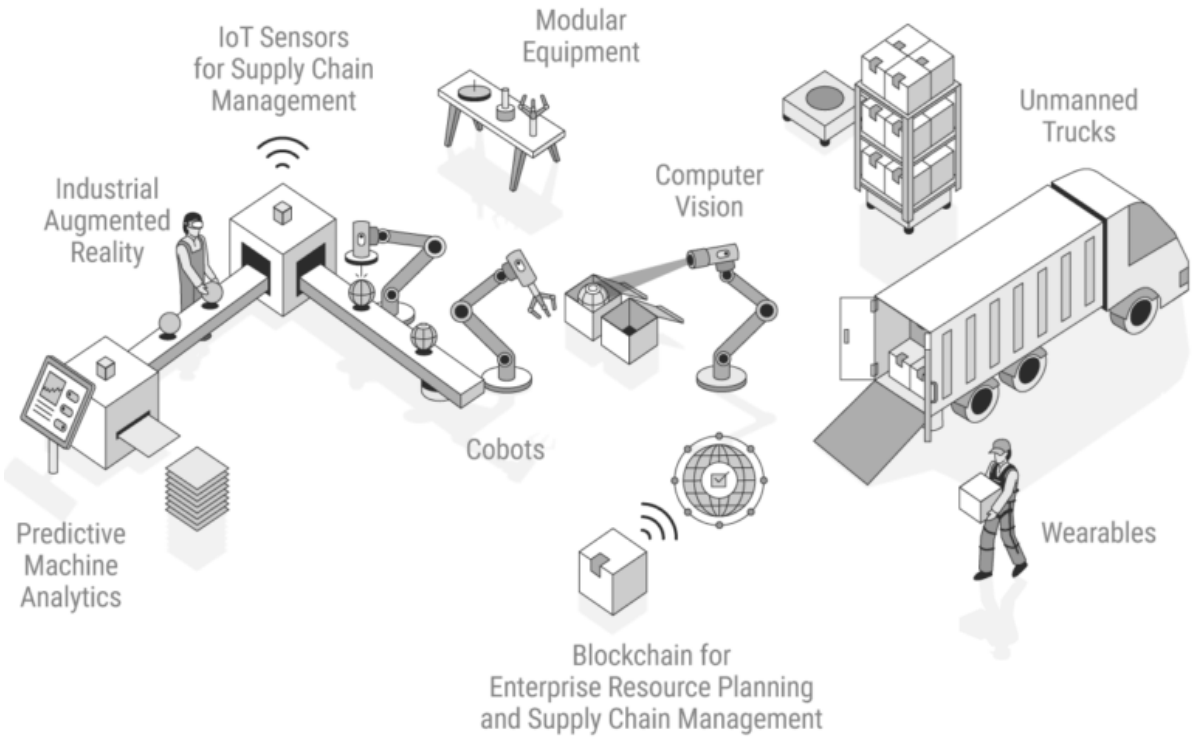


Figure 3-1 IoT in a manufacturing industry (50)

Furthermore, factories employing blockchain will be better positioned in the event of a recall. In factories where food or automobiles are processed, a single system for managing recalls could more swiftly figure out the origin of faulty parts or contaminated batches, potentially saving lives and money (46). In the future, blockchain technology should make organizations more autonomous this given that its consensus mechanism, allows participants to carry out decision-making without depending on a central entity. Furthermore, blockchain enables product and asset movements more digitized and trackable in real-time. In general, distributed ledger technologies, not only promise to simplify supply chain management but also enhance the transfer of information in a safer way, generate a decentralized government, make payments frictionless, among other aspects that will be detailed below.

In *Table 3-2*, the general aspects with which blockchain technology could strengthen and contribute to an IoT network are described.

Aspect	Blockchain contribution
Decentralization	A shift from a centralized architecture to a distributed one could remove central points of failures and bottleneck. For the daily user, decentralization provides them the ability to exert control over their data, rather than give it to centralized corporations who could claim ownership of it (11).
Identity	Immutable data stored at the blockchain provides identity to every single device in the network. A trusted and distributed ledger will provide also authentication and authorization processes for the devices enhancing the network of IoT (10).
Autonomy	An IoT network based on blockchain is enhanced with the smart contracts universe, where a simple sensor can become a decentralized autonomous corporation [20](DAC). DACs are able to take decisions and have an autonomous interaction with the environment (machine to machine and person to machine) (11).
Reliability	The immutability of the data distributed among the chain and the possibility of the participants of the network to verify each historical transaction of the chain gives to the network the certainty that it has not been tampered. Reliability is a key aspect of the blockchain to bring in the IoT (5).
Security	All the transactions in a Blockchain network are secured by strong cryptography. Furthermore, the transparent nature in the case of blockchain makes it secure and auditable as everyone on the

[20] A decentralized autonomous organization (DAO), sometimes labeled a decentralized autonomous corporation (DAC), is an organization represented by rules encoded as a computer program that is transparent, controlled by shareholders and not influenced by a central government

	network knows about all the transactions and the transactions cannot be disputed (9).
Market of services	A distributed ledger technology can accelerate the creation of an IoT ecosystem where transactions between peers are made without the need of central authorities. Transactions as micropayments can be made in a trustless and reliable environment (5).
Secure code deployment	The immutability and security of the blockchain provide the necessary safety of the code deployment into the devices. Manufacturers can update and track the code with the highest confidence. Therefore, devices can be updated securely through IoT middleware [21] using blockchain (11).
Leadership and Governance	The blockchain economy challenges established notions of governance with a new kind of governance, called a Decentralized Autonomous Organization (DAO). Implicit and explicit contracts are managed by blockchain. Records are decided in a decentralized way through consensus. Potential to reduce the coordination costs of economic activities (12).

Table 3-1 General blockchain technology contributions to an IoT network

Briefly returning to the current operation of the IoT architecture, the biggest challenge in IoT security comes from the ecosystem architecture itself, which is based entirely on a centralized Server/Client model. All devices are identified, authenticated, and connected through servers in the cloud that support mass storage and processing capabilities. The connection between devices must be through the cloud, even if they are only a few meters away. Although this model has been interconnecting generic computing devices for decades and continues to support small-scale Internet networks, it will not be able to meet the growing needs of tomorrow's huge integrated circuit ecosystems.

Cost is another major hurdle, particularly for the use of such a centralized model in the development of existing solutions. The high cost of infrastructure and maintenance is associated with centralized clouds, large server groups, and network equipment. The huge amount of communication that should be handled when the number of integrated circuits devices goes up. However, even if the extraordinary challenges of the economy and industrial production are overcome, each block of architecture would have a bottleneck and a potential site of failure that could disrupt the operation of the entire network.

Blockchain is still far from widespread implementation. Nevertheless, in many sectors, the significant benefits it offers are already being exploited. Since blockchain is a peer-

[21] Internet of Things middleware is software that serves as an interface between components of the IoT, making communication possible among elements that would not otherwise be capable.

to-peer (P2P) network within a system, the time and costs of intermediaries are significantly reduced. This ability to eliminate intermediaries greatly facilitates its viability and implementation, a need that the company has been demanding for some time in any type of transfer. The structure of current systems greatly disadvantages small competitors and small businesses who, through this decentralized system, gain a much more equal position in their favor.

3.1 Use cases

Below are some use cases that are developing blockchain technology to improve current systems or create new business niches.

Sector	Blockchain application	Companies
Supply Chain and Logistics	Many stakeholders are involved in a global supply chain network. IoT combined with blockchain can help enhancing the reliability and traceability of the network, collecting data through devices that will be providing information about weather conditions, movements, speed, general status, etc.	Worldline, Marsk+ IBM, Everledger
Automotive Industry	Automotive industries are using IoT enabled sensors to develop fully automated vehicles, enabling multiple users to exchange crucial information easily and quickly. Possible uses: automated fuel payment, autonomous cars, intercommunication for traffic control, smart parking.	Renault, Volkswagen Microsoft
Smart Homes	Traditional centralized IoT devices allow people to control remotely different parameters of their homes or control their electronic equipment. Blockchain would allow decentralizing functions, as well as providing user privacy and increasing network security.	Telstra
Sharing Economy	With the recent emergence of the shared economy (motorcycles, cars, bicycles, skateboards, apartments, etc.), a blockchain network that both parties trust would allow for example the use of devices that are leased alone without the need for a third party, that monetizes part of the transaction.	Slock.it, Origin, Sharering
Pharmacy Industry	Transparent and traceable information about the origin of the medicines storing the data on a blockchain can reduce tries of counterfeit. This use case would be a more specific case of the use of blockchain in the supply chain.	Mediledger
Agriculture	It is possible to improve the agriculture using IoT sensors in the farms that would provide reliable real-time data (reliable if the IoT network is decentralized) about the climate conditions taking needed actions to have an ideal growth of the plantation. The information could be also available for final customers that could verify the characteristics of the	Pavo IoT Oxfam Aon

	product that they are buying. Blockchain is also being used to provide automated microinsurance to small farmers	
Insurance	Blockchain can make data transmission between the insurer and the insured less expensive and faster, also allowing automatic payment of insurance policies. In addition to the use of reliable IoT devices, fraud attempts are also reduced. The world's leading insurance companies have already created the B3i consortium to study and develop blockchain technology in this regard.	B3i

Table 3-2 Some IoT-blockchain current use cases applied by companies

As already mentioned in the IoT section, the number of IoT devices is increasing exponentially as people are adopting them and understanding their benefits. To reach such growth, IoT devices need a network that is capable of supporting all the information that is transmitted between the devices, with standardizing protocols, proper layers, and adequate structure. Current network solutions rely on centralized servers, where the data is transmitted between the device and a cloud server through the internet. Although this option may work the exponential expected growth of IoT devices raises the need to try new alternatives that can offer advantages over a centralized network, since the greater the growth of the network, the greater its exposure to security failures and the greater the cost of the data breach.

Even though in the past, some decentralized structures have been tested to support the network as peer-to-peer wireless sensor networks (50), still these networks do not provide high levels of security and trust. That is why blockchain stands as a promising alternative P2P in the field of security because it is immune to any tampering, as it is highly encrypted using advanced cryptography in a decentralized way, being a solution for the centuries-old consensus problem. The next section presents the security aspect and how it can contribute to an IoT ecosystem.

3.2 Security and privacy scandals

Blockchain is a technology by nature decentralized, however, it is not safe only because of that. Its security lies in aspects such as cryptography, its data encryption, and the consensus mechanism that prevents malicious participants from violating the data, and consequently, the security of the system. In this section, certain examples will be exposed where aspects such as privacy and data security are violated. Among these examples are the scandals such as the personal data of the users exposed by Facebook or the terrible hacking by the UK public health network.

It is hard to imagine the day to day of people without the interaction with an IoT device. It is correct to say that in the future the world will be increasingly interconnected given the continuous communication of intelligent devices. However, security represents only one of the important problems that affect these devices. IoT

devices and networks are still very insecure while data protection and privacy are not assured. Among the historical records of serious vulnerabilities or attacks on the safety of these control of cardiac devices[22], the disablement of vehicles [23] and the largest DDoS attack in the world[24] can be mentioned.

In the information systems, there are three basic requirements to guarantee the security of it:

- Confidentiality: to protect the data from unauthorized accesses.
- Integrity: to provide trusted data that cannot be modified or deleted by unauthorized parties.
- Availability: the data should be accessible when needed.

In a traditional IoT architecture, the transmitted data is managed in a central location such as a farm of servers or a cloud (48) (33). While the administrators of the infrastructure remain trusted and the network is not being affected by malicious attacks, the approach of a centralized architecture is valid. However, since the data is stored in a central entity, such as a cloud server, security is based on a single entity that can be an easy target to attack by hackers. In a decentralized approach, composed of many nodes that support the network and work as validators of the data transmitted, even if a node gets compromised it does not affect the working of the whole network. These nodes, together, can store and transmit certain important information about IoT devices such as their identity, the permits they have, or any other information that needs to be protected. Such information would flow in parallel to the traditional network of IoT devices and could be required at all times by IoT Devices if they meet the access requirements.

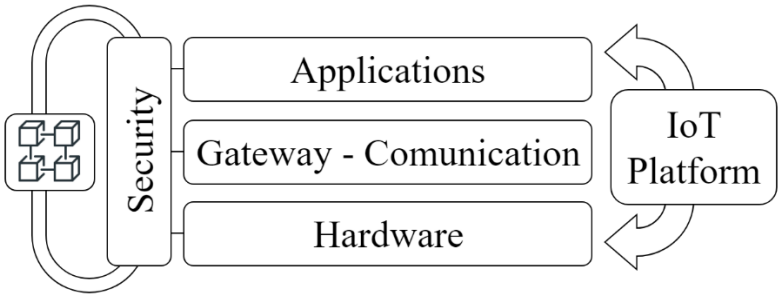


Figure 3-2 Scheme of a blockchain storing data from an IoT network.

[22] The Food and Drugs Administration organization of United States confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks.

[23] The IBM security intelligence website reported a Jeep hack a few years ago. In July 2015, a team of researchers was able to take total control of a Jeep SUV using the vehicle's cars internal computer network.

[24] In October of 2016, the largest DDoS attack ever was launched on service provider Dyn using an IoT botnet. This lead many actors of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN.

Security

Any security flaw in a traditional IoT ecosystem can expose compromising information about users. One point that is not always considered in IoT devices is their longevity. Most do not have the necessary hardware or software to update themselves in a secure and remote way, so with the years and the loss of updates, hackers can discover gaps and access to them. Lack of trust and transparency is a problem that worries people more and more. Next, certain cases where the security of networks of IoT devices have been compromised by computer attackers will be exposed.

FancyBear attack: Microsoft Threat Detection Center issued a warning on its official blog on august 2019 (51): the Fancy Bear hacker group, which has unofficially associated with the Russian cyber arm and secret services, has been attacking devices connected to the Internet of Things (IoT) to make intrusions in the networks to which they have been directed.

According to Microsoft, the wave of attacks on IoT devices was first detected in April of 2019 during the analysis of an IP phone, a printer, and a video system. Hackers have taken advantage of the fact that at least two attacked devices have easy-to-discover passwords and a known defect in proprietary software. The three devices had in common that allowed control from a remote network (52).

Silex malware: it was created by a 14-year-old hacker to erase the firmware of devices such as surveillance cameras, locks, light bulbs, thermostats, routers, webcams, and in general connected products from home or office. The malware can erase all storage of IoT devices, remove firewall rules, network settings, and completely kill the device. Deleting the firmware is the most destructive thing that can happen to an IoT device since the following would be to burn its circuits. For the device to work again, users must manually install the firmware and reconfigure from scratch, a complicated task for most users, so in this case, many users would end up discarding the devices (53).

Brickerbot malware: in the first four days of operation, Brickerbot malware managed to attack a total of 1,895 devices, while on the fourth day it attacked about 1,400 devices in just 24 hours. The malware scans the Internet to find IoT devices in which it tries to access through "serial" passwords that manufacturers include in their products so that users can access their settings. From there they erase the memory of the devices, corrupt their storage systems and disconnect them from the internet. Subsequently six months later, the creator announces that his malware would have infected more than 10 million devices. The creator of BrickerBot explained that his malware is an "Internet chemotherapy", and confesses that he hopes he expects this to help minimize the number of distributed denial-of-service (DDoS) attacks (54) (55).

Dyn cyberattack: on October 31, 2016, the Dyn cyberattack took place. Dyn is a US-based company that works as a Domain Name System (DNS) provider. The attack type was a distributed denial-of-service (DDoS) which left large platforms and Internet services inaccessible to many users in Europe and North America (56). Dyn reported that the attacks originated from "tens of millions of IP addresses" (57) where many of these IP addresses came from IoT devices like baby monitors, home routers, digital video recorders, webcams, among others (58). The process of the attack was as follows: the first victim received a phishing email that, by accessing it, allowed the virus to spread to other devices connected to its networks such as video cameras, printers, or other IoT devices (11). These devices were subsequently used to generate the DDoS attack on the Dyn company. Since the information on IoT devices is currently connected to the cloud, security depends entirely on a central point and consequently the risk of a single point of failure.

The above represent only some of the malware and attacks that have violated the security of current IoT devices. As can be seen, as IoT networks are growing and becoming more relevant, the greater the interest of hackers in violating the security of these devices. There are many types of attacks that an IoT device can suffer (6), so increasing its security is essential. Although at the moment there have been no significant attacks in terms of damage (at least compared to the attacks of ransomware to computers or computer networks), these detections of security failures and first attacks, are proof that the security in the networks IoT is being tested. If in the future, IoT networks will be part of daily life and will address such important issues as the health of people or confidential data of people and companies, security must be paramount. It will be mentioned below, one of the most famous ransomware[25] of recent times, which caught the attention of much of the world press. Although the attack was carried out on computers (which are not considered IoT devices), it shows the real danger that such an attack can mean, for example, to IoT devices that are dealing with data or actions on the lives of patients in hospitals.

WannaCry Hack: the so-called WannaCry hack shut down hundreds of thousands of computers around the world. The attack began on Friday, May 12, 2017, and has been described as unprecedented in size, infecting more than 230,000 computers in more than 150 countries (59). The global cyberattack halted computers in hospitals across the UK and cost the NHS[26] £92m, a report from the Department of Health has found. (60). Hospitals rejected patients and canceled appointments after being infected by the

[25] Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

[26] National Health Service in England.

ransomware, which encrypted computer data and demanded payments to restore access.

During and after the attack, evening and weekend clinics in general practitioner (GP) practices were impacted due to the lack of availability of electronic patient records and clinical systems. NHS England did not collect data during the incident on how many GP appointments were canceled or how many ambulances and patients were diverted from the accident (61). The ransomware was so powerful that even government authorities indicated that it should have been developed by some organization supported by a country (62).

Privacy

Next, one of the most meditative scandals of recent times regarding the violation of user privacy is briefly described. Even if it does not belong to the category of attacks on an IoT network, it allows us to understand how data theft can be used for purposes other than those authorized by the user. It is not difficult to imagine in the future, for example, use of the data of wearable devices, our vehicles, or the IoT devices of our house to generate a database that stores people's data and uses it for purposes not consented to by them.

Facebook scandal: in the year 2014, Cambridge Analytica got the permission of Facebook to request data from its users and thus perform a study about people's personalities. The users had to fill in a small questionnaire and in return, the users received a small amount of money. Of course, all this voluntarily. Cambridge Analytica put $ 800,000 and through this method got some 270,000 people involved. Thanks to this method they were able to collect data about their tastes, location, religion, political opinion, identity, etc.

When this study was conducted, in 2014, Facebook allowed data from your contacts to be sent (if they maintained the privacy settings that come by default). This is how they managed to multiply the 270,000 users by 50 million. Facebook would later recognize that Cambridge Analytica violated the platform's policies by accessing the data of nearly 50 million users without their consent. Two years later, the same company, would work as a consultant for the presidential campaign of Donald Trump, using user data for political campaign purposes.

The controversy generated by Cambridge Analytica on Facebook was only the tip of the iceberg. After the Facebook scandal, new problems related to Facebook over the treatment of users' information and their privacy users have been emerging.

3.3 Incorporating blockchain into IoT security

It has already been mentioned that the structure of the blockchain provides greater security due to the fact of being of a decentralized nature, its cryptography, and encryption. These features can be complemented with existing security mechanisms or structures to improve the defense capacity of the systems. As already mentioned, the centralized architecture of the systems, in general, makes them vulnerable to attacks that should only focus on violating the security of that central entity. In the case of IoT architectures, when all work with a cloud connection (even though Fog computing and Edge computing do so to a lesser extent), they also become vulnerable in this aspect. At present, attacks on an IoT network have already been registered, such as the one in 2014 where the security of more than 100,000 IoT devices saw their security compromised by sending around 750,000 emails of phishing and spam (63). The change of architecture of a centralized one towards a decentralized one is the vision that the inclusion of the blockchain proposes.

Below are some aspects where a blockchain can strengthen an IoT network:

- Insights from the blockchain can be used to track the sensor data and prevent duplication with malicious data.
- It can provide each IoT device with a unique identification, authentication, and seamless secure data transfer.
- A generalized platform like blockchain may be used by all IoT devices to communicate with others. This will reduce costs as a third-party facilitator will no longer be necessary.
- Provide a history of connected devices for troubleshooting purposes

As long as the problems of scalability, interoperability, and consensus are not completely resolved, hybrid solutions will be a plausible solution, taking advantage of the benefits of the blockchain and maintaining the traditional IoT architecture when required.

In the past, companies used to keep their data stored locally, which led to high maintenance costs and the need to have their servers. Currently, the data storage and maintenance of the servers is given by specialized companies that provide the service through the cloud, however, these companies represent a central authority that manages and controls all operations of the communicating nodes (usually cloud-based) and the future, where after integrating blockchain no central authority would be needed for data management, reducing the problem of a single point of failure. The foregoing, which generally describes data storage structures, can be applied to IoT networks, which also require the transmission and storage of information. Figure 3-3 shows how IoT structures could go from a current centralized structure to a decentralized one.

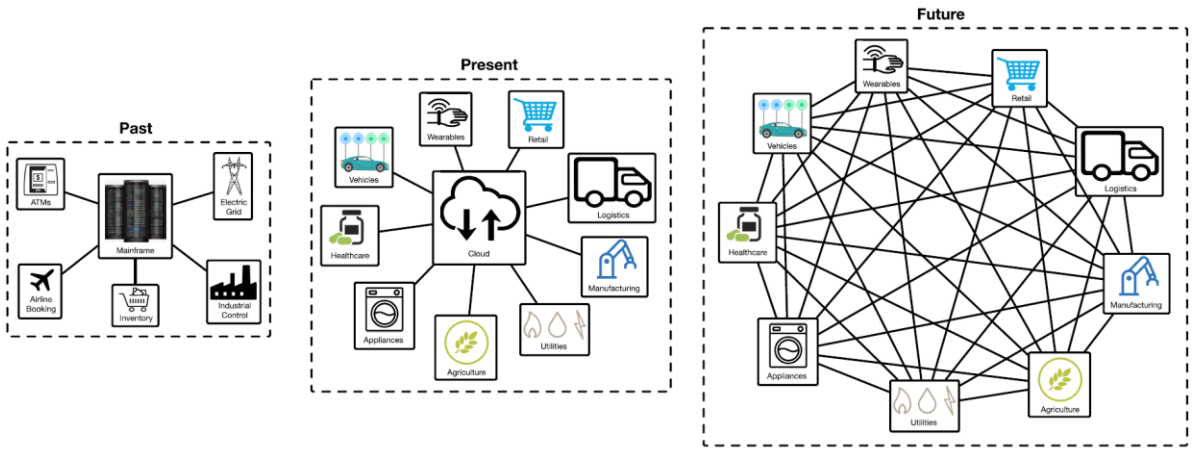


Figure 3-3 Centralized and decentralized systems in IoT architecture (18)

3.4 Types of IoT architectures enhanced with blockchain

In the integration of the blockchain into an IoT architecture, many alternatives can be generated to strengthen the security and privacy of the system. As in IoT architectures, the detailed structure depends on the needs of the system, the same is true for an IoT-blockchain ecosystem, so each company is likely to design its unique ecosystem. However, for the general classification, the approach carried out by A. Reyna et al. stands out, where they classify a Blockchain IoT ecosystem in three general types (5).

IoT-IoT: this alternative could be one that has less latency time and better security because it can work offline. Only some specific data would be stored in the blockchain but the communication between the devices (interactions) would be done without the use of it. This scenario would be appropriate when reliable IoT devices were used and high speed is required in terms and latency. In *section 3.5*, a specific case is shown where blockchain is used to authenticate the firmware of an IoT device.

IoT-Blockchain: in this scenario, all information transactions between IoT devices would be stored in the blockchain. The information stored in the blockchain is immutable, so this alternative is for those systems in which the information shared between IoT devices should not be deleted. One case would be for example the traceability of the use of transport vehicles for autonomous leasing (sharing economy, for example, Slock.it), to store in the history the usage data as well as those of its user. However, as will be detailed later, the use of the blockchain to store all the data can mean an increase in bandwidth, this being one of the challenges of the technology in the face of the constant increase of information to be solved.

Hybrid approach: In this scenario, unlike IoT-IoT, in addition to information about IoT devices, part of the interactions are also stored in the blockchain (for example, those of lower frequency), while the rest of the interactions do not. The dilemma is in

choosing what kind of interactions are stored in the blockchain and which are not, as well as who decides it. In this scenario, technological advances can be used in terms of IoT network architecture such as the aforementioned Fog Computing. For example, transactions of devices with high battery capacity or those connected to the network could be recorded, while those devices that have limited capabilities (low-powered devices) would use an IoT architecture of the FOG type.

The representation of the 3 scenarios described above is in *Figure 3-4.*

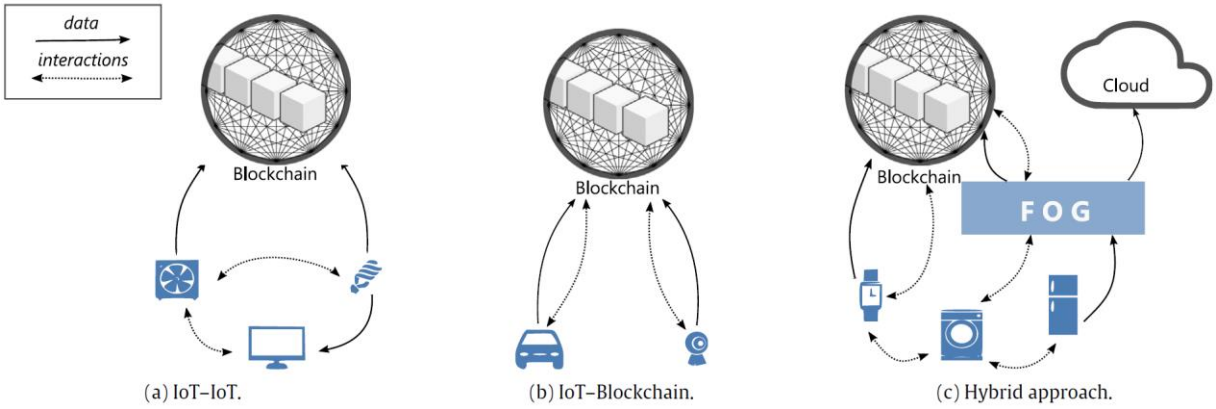


Figure 3-4 IoT and blockchain ecosystem, possible interactions (13)

Explained the possible general architectures of an IoT system for interactions between IoT devices using blockchain, in the next section case of use of an IoT-IoT architecture is shown. The two cases of use explore the use of blockchain for the specific case of firmware[27] and datasets identification

3.5 Blockchain case of use for firmware detection

No security system is impenetrable, so every IoT could be compromised despite the security measures. As a general rule, the weakness of any system lies in its weakest link. In this section, (13) propose a self-healing system that could be designed using Blockchain to repair the compromised systems. The next case of use is proposed by M. Banerjee et al. to enhance the security of the firmware detection of any device.

In the traditional technique, the integrity of the operating system of the device is checked every time before its execution by the bootloader[28]. The bootloader is stored in a partition with a read-only option, so it is not possible to modify it. Similarly, the operating system checks the integrity of applications before launching them usually comparing the integrity metric of the apps with the Reference Integrity Metric (RIM). The RIM is stored in a safe place and pre-loaded by the official company, which is only modified on certain occasions with a firmware update. So, if the RIM is compromised

[27] In computing, firmware is a specific class of computer software that provides the low-level control for the device's specific hardware.

[28] Small, often unmodifiable code and data that controls hardware devices.

during a firmware update, the verification system will fail and allow the compromised firmware to be loaded. It is therefore in these updates, where a system vulnerability can be found. In this case, (13) propose using blockchain technology to improve RIM protection. *Figure 3-5* shows the proposed scheme. In this case, the RIM would be stored in a blockchain and would be shared by all devices of the same model or that occupy a certain version of the software. Therefore, in the case that only one device was affected, it would be easily detectable since the rest of the devices would maintain the original RIM. Just as a transaction is verified by all the nodes of the blockchain network, in this case it would be done with the RIM, so the attacker should be able to control at least half of the devices to corrupt the blockchain and thus the RIM history record (assuming, for example, a PoW consensus mechanism in the blockchain).

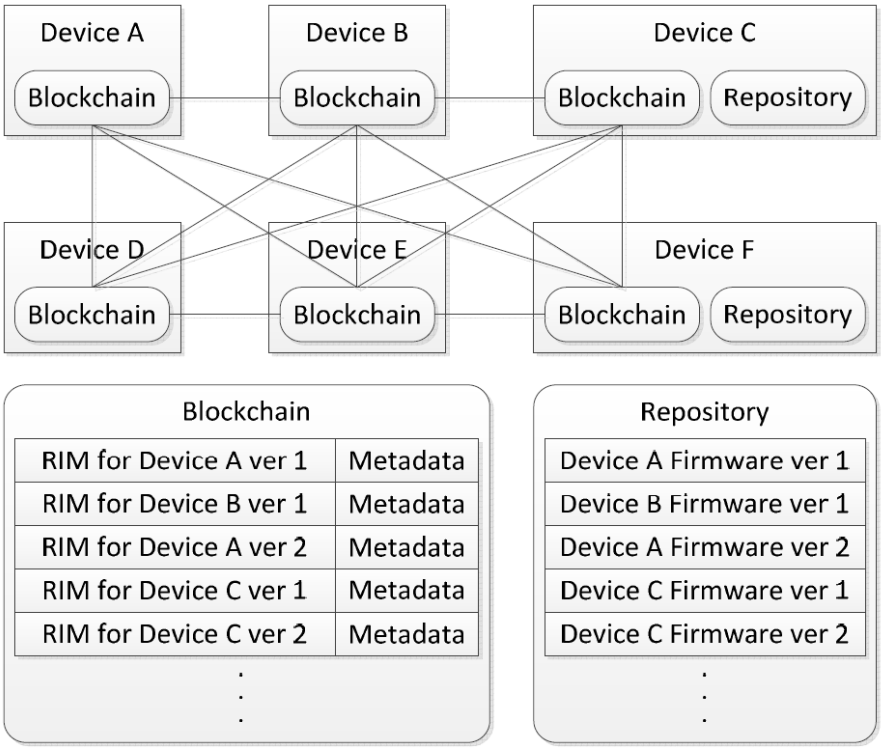


Figure 3-5 Blockchain-based compromised firmware detection and self-healing (13)

Thus, in the case that only one computer was compromised, and the RIM was modified maliciously, the blockchain would maintain the original RIM and also show the new corrupt RIM. To heal a corrupt software, new code or the original code replaces the corrupted one. Therefore, the compromised firmware using blockchain, the corrupted firmware could force to roll back to its previous version using a smart contract for example. Since IoT devices are connected to a network, they can be updated remotely. After the authentication process of the update for the firmware, the metadata, the new version of the software, and the reference integrity metrics are stored in the blockchain. The challenge of the proposed system is to define the legitimate firmware update procedure through a debug interface or a remote entity. Any type of firmware update

must be handled by hardware modules for self-healing. Once the update is authenticated, the automatic recovery logic receives the new firmware through a debug interface or a network (13).

3.6 Blockchain case of use for dataset identification

In the security solution presented by M. Banerjee et al. (13) for a dataset sharing case, blockchain is used to ensure the integrity of shared datasets and the IoT system. In the proposed system, to ensure the integrity of datasets[29], a reference integrity metric (RIM) for the dataset is maintained using the Blockchain, that way the integrity of the information could be checked every time using the RIM. In this approach, there is a central hub that maintains the references of the member repositories (where the datasets are stored and distributed). Information such as the owner, the address, and sharing policy is maintained by the Blockchain. Another Blockchain ensures the integrity of datasets, maintaining the RIM of datasets. It is important to consider that many times, not all information must be disclosed.

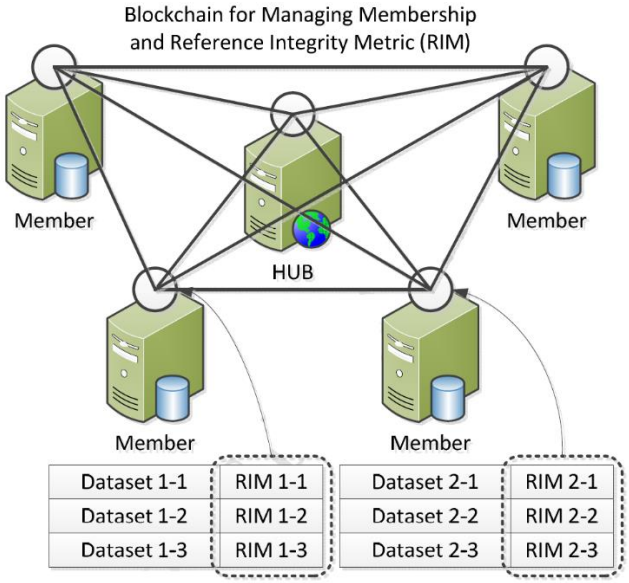


Figure 3-6 Blockchain-based management of membership and reference integrity (13)

For many organizations, it is important to preserve the privacy of certain information such as in cases of confidential information. The same happens in the case of users who wish to make public only certain data while maintaining privacy in the rest. To achieve the above, M.Banerjee et al. emphasize the need for an automated system that

[29] A dataset is a collection of data. Most commonly a data set corresponds to the contents of a single database table, where every column of the table represents a variable, and each row corresponds to a given member of the data set in question

anonymizes certain datasets that require it before being released (13). Moreover, there is an important aspect that should be taken into consideration. When information is recorded in the Blockchain it cannot be erased, so in the case that the datasets are not suitable to be shared permanently they could not be erased if they would be stored in the blockchain. That is the reason why in the proposed scenario, only RIM is maintained by the Blockchain so this way datasets could be stopped from being shared without any problem because only the RIM will be at the blockchain while datasets could be erased when needed.

The case would be analogous to use blockchain for the identification and authorization of IoT devices where instead of using the RIM to identify the dataset, it could be used to identify the IoT devices.

3.7 IoT-blockchain initiatives at the industry

In the present, many companies around the world have been investigating and implementing a wide variety of measures using blockchain to strengthen IoT network security.

IBM: the company is leveraging its cloud infrastructure with blockchain to provide tracking services of high-value items (11). Select data is managed, analyzed, and customized to share among permissioned clients and partners. The data is allocated in distributed records, maintained by consensus, and cryptographically hashed. The IBM platform, called Watson IoT, is based on a blockchain model as a service and is based on the open-source Hyperledger Fabric[30]. The platform ensures that it enhances security, enables the inclusion of low-value devices, and ensures easier long-term device management (64). The platform translates data from connected devices into the format for the smart contract required by the APIs. There is no need for the blockchain smart contract to know the details of the device data, thus, enhancing privacy. The platform filters the events of the device and sends only the data necessary to fulfill the contract (11).

Volkswagen: it is one of the few automotive companies that have begun to accept and experiment using blockchain and other distributed ledger technologies. The firm has formed a large number of partnerships with companies linked to the blockchain to take advantage of the enormous potential it offers for the automotive industry. For example, they work with Minespider[31] on a pilot plan to track the supply of lead from the automaker using Blockchain to guarantee that its raw materials are obtained in a socially and environmentally sustainable way. Blockchain records will allow the raw

[30] Hyperledger Fabric is an enterprise-grade permissioned distributed ledger framework.

[31] Minespider is a blockchain protocol and DApp for tracking responsibly sourced raw materials in the supply chain.

material to be traced to its point of origin with Digital Certificates (65). Volkswagen's latest move has been to partner with the IOTA project, a case study explained in *Chapter 7*, which is a non-profit organization and one of the most popular initiatives of DLTs in the field of IoT. The goals are the registration of over the air update (OTA) records on an immutable data storage. In the IOTA distributed ledger technology proposal (Tangle), data integrity can be ensured to prove interoperability and production readiness in the different areas of communication exchange that require it as on-demand features, vehicle to vehicle (V2V) and vehicle to infrastructure (V2L) communications (66).

Porsche: the German car company, has been conducting tests of an automatic payment system using blockchain for parking to eliminate the user's need to pay to a physical location. The system works as follows: the customer drives his car to a parking lot, which has a radio frequency building (RFID) device. Through electromagnetic waves, the parking lot obtains the necessary information. When the client leaves the parking lot, the identification is transferred again and the parking fee, which acts as an IoT device, sends the information to the client's virtual blockchain portfolio, where a block of information is generated to document the transaction. This way it is not necessary for the customer to walk to the parking ticket machine or look for the exact change to pay (67).

HYPR: the company provides a decentralized biometric tokenization system that provides companies the ability to replace the use of centralized password-based systems (68). The company aims to deliver biometric security to the world of digital and physical assets such as Intellectual property, ATMs, cars, smart locks among others, by forcing malicious hackers to divert the attention from a centralized validation server to many client-side devices (69). Creating biometric tokens[32] enhanced by blockchain reduces the viability of an attack by decentralizing the points of attacks. The system works as follows: sensitive information related to security authentication such as fingerprint image, voice, or facial data is divided and encrypted in small packages of data represented by tokens. These tokens no longer contain all the sensitive information and their information is validated by a series of additional security layers, so it is very difficult for the attacker to fail to obtain all the necessary information to carry out an effective theft of information.

[32] Tokenization is the process in which sensitive information is replaced with a randomly generated unique token or symbol. By using tokens instead of the actual information, the risk of theft is reduced considerably because the data is useless if it's intercepted or accessed by malicious actors.

4 Blockchain challenges

Currently, IoT devices are being designed to fulfill their basic tasks, so the processing power and energy storage capacity of many of them is limited. In general, IoT devices are low-powered devices, with microcontrollers of 8 or 6-bit, small amounts of RAM, and storage capacity (7). Blockchain technology provides a decentralized network, improving security and privacy that could enhance an IoT network. However, first blockchain developments involve a significant delay in the communications, significant consumption of energy, and computational overhead that is not suitable for most IoT devices that have limited resources (8).

4.1 Energy efficiency

The main blockchains (as Bitcoin or Ethereum) use the Proof of Work (PoW) as a consensus mechanism. While it is true this confers extreme security to the network, it is no less true that miners consume large amounts of energy to keep distributed computer networks running. According to Digiconomist Bitcoin's energy consumption index (70), currently, the bitcoin blockchain (that uses PoW) consumes as much electricity (73.12 TWh) exceeding the electricity consumption of countries such as Austria, Switzerland, the Czech Republic or Colombia. Of course, it is true that such consumption is given because the miners have been increasing their mining capacity in the network and therefore, increased electricity consumption. However, in an IoT network with an increasing number of nodes connected to the network and in where every IoT device would be involved in the blockchain PoW process, energy consumption would be a problem. Moreover, considering the battery life constraint of many IoT devices, a blockchain using the PoW algorithm, by itself, would not be suitable for small IoT devices with low battery capacity.

Although the PoW consensus mechanism is not ideal given that all the nodes involved would mean a large energy expenditure, there are other approaches (71) that would allow this problem to be avoided using blockchain with PoW with parallel sub-blockchains that would allow the network to be scaled without excessive energy use.

4.2 Scalability

To get decentralization and immutability, blockchain suffers from scalability and speed issues. This phenomenon is called the Decentralization Consensus or Scale (DSC) trilemma theorem. The theorem exposes that blockchain can achieve only two of the following three properties in a distributed system decentralization, security, or scalability. Given the above, in a highly decentralized and secure public blockchain, scalability is a problem. For instance, scaling capabilities can be achieved by sacrificing the decentralization attribute of a blockchain. Such an approach is pioneered by Delegated Proof-of-Stake (DPoS) blockchains, such as Bitshares and EOS. The

following image represents the scalability trilemma, where to maximize the characteristics close to each side of a triangle, you have to sacrifice the third remaining element.

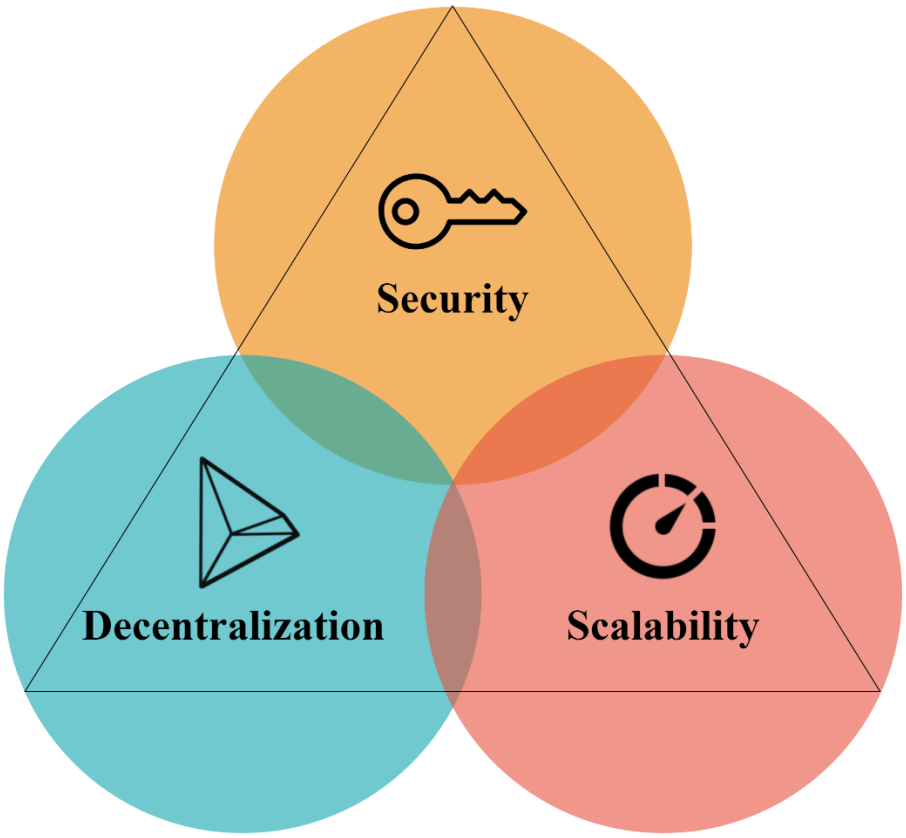


Figure 4-1 Scalability trilemma

The triangle considers scalability, decentralization, and security in fault-tolerant consensus protocols. Depending on the blockchain metrics, it can be focused on some of the three parameters. For example, Bitcoin's blockchain sacrifices scalability in exchange for decentralization and security, which has made it incredibly robust over the years. Scalability is a critical component for the mass adoption of blockchain to face traditional IT operating the business. Being able to compete with the traditional IT alternatives, blockchain networks will be also offering the benefits of a distributed ledger technology.

From here a small conclusion can be drawn. In a single blockchain, there are several factors that will affect the performance and it is not possible to have all the factors at their optimum level, there is a trade-off between them. For example, Bitcoin's blockchain is considered one of the most decentralized and secure blockchains of today, given the hundreds of thousands of miners that support the network and the thousands of nodes that maintain the ledger.

4.3 End-to-end reliability

It has already been mentioned that the information stored in the blockchain is immutable, secure, and trusted. However, what happens if the information that enters the blockchain is in itself wrong? This is a challenge that has been posted in recent times, and it is called the end-to-end reliability. Smart contracts are considered secure and reliable, but to keep these characteristics, it should be assured that also the information that enters and exit the smart contract, is conserved over time and outside the blockchain borders where a smart contract exists. Therefore, the inputs and outputs that the contract relies on also need to be secure.

Smart contracts require secure middleware which works as a bridge to the real-world data. In order to reach a secure middleware or network of IoT devices to provide information for the blockchain, decentralization outside the main blockchain is also needed. Another problem is the interoperability of smart contracts executed on the blockchain. The interoperability of smart contracts is necessary to achieve a safe and compatible execution between the different blockchains. Both problems mentioned above are faced by the case study that will be presented in the next Chapter. Chainlink is a blockchain middleware company that introduces an ecosystem that seeks to decentralize oracles as well as provide interoperability to smart contracts.

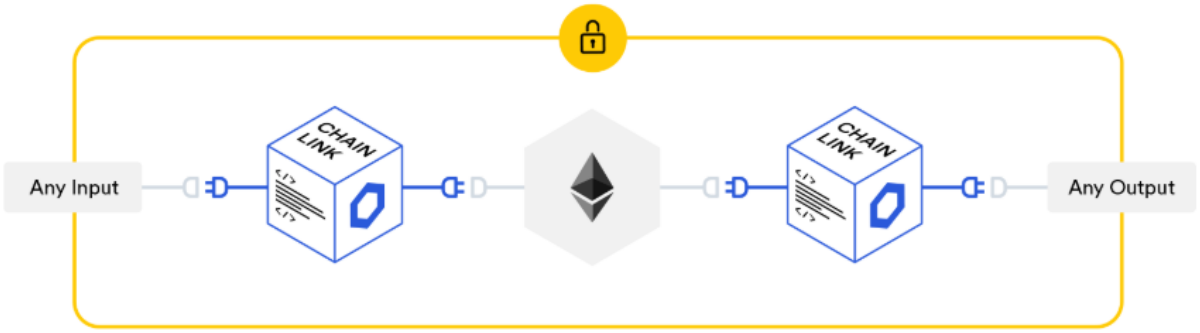


Figure 4-2 End-to-end reliability representation (15)

4.4 Interoperability

Despite all the benefits that blockchain brings to the internet and therefore to the internet of things, blockchain technology needs to address challenges that stop its potential to enhance internet data storage and communication. As the blockchain industry continues to grow and progress and many blockchains are coming into space with different proposals and advantages, interoperability will be an essential feature. Currently, most of the blockchains are not able to "communicate" with each other and share data, therefore interoperability must be faced. Several blockchains focus on certain attributes such as high scalability, security, ease in creating projects (being compatible with multiple programming languages), and other features. However, interoperability between blockchains is an area that remains in the background. A

theoretical real case would be a car company that decides to use a blockchain to connect vehicles, enabling communication with each other obtaining all the benefits that the blockchain offers. Depending on the blockchain used, these vehicles could not interact with vehicles of another brand that has decided to use another blockchain, since blockchains cannot currently connect with each other.

Even if many projects aim to provide solutions to the users few also worry about being compatible with other blockchains. For example, IBM Hyperledger Fabric is excellent for supply chain management, while Corda de R3 is the best choice for financial sector solutions. But when it comes to connecting applications that work in both blockchains, thus, sending and receiving data between them, it is not possible. The platforms concentrate their efforts on offering better performance than the other blockchains, so they neglect the goal of being compatible with their competitors. However, although in general blockchains do not offer interoperability by themselves at the moment, there are alternative solutions that are being developed, which will allow them to connect both blockchain and achieve interoperability (72).

It is inefficient to have hundreds of blockchains completely separated from one another. To take advantage of the full potential of the smart contracts and the strengths that can be found in different blockchains it is a need to transfer the information from one blockchain to another. As innovation is generated in different aspects, the need to connect blockchains arises to solve some of the problems that have been mentioned before as scalability and compatibility. An important point proposed to achieve interoperability, is the cross-chain smart contracts. This is possible because cross-chain smart contracts enable several blockchains to communicate with each other and function as a single chain.

4.5 Connectivity

A new technical challenge arises with the smart contracts' trust model: connectivity.

In the field of blockchain, the first development that is carried out is to create developer-friendly platforms so that they can easily create applications in the blockchain (decentralized applications) as well as smart contracts. However, the challenge of connecting these applications with data sources that already exist today and that are based on different protocols must be faced. For example, a lot of the data collected in the real world is provided by data feeds and APIs, being external to the blockchain. The solution to this problem is to introduce new functionality called an oracle[33] that provides data to the blockchain. Oracles feed the smart contract with

[33] An oracle, in the context of blockchains and smart contracts, is an agent that finds and verifies real-world occurrences and submits this information to a blockchain to be used by smart contracts

external information that can trigger actions of it. However, the so-called oracles are exposed to a point of failure also since they have a centralized architecture. Any smart contract using a blockchain that relies on data provided by centralized oracles has a single point of failure, being no more secure than traditional centrally run agreement (15).

There are different types of oracles (73):

- Software Oracles: collect information available from online sources like temperature, price of commodities, transport schedules, etc.
- Hardware Oracles:
    - Inbound Oracles: Provide data from the external world. E.g humidity sensor
    - Outbound Oracles: Provide smart contracts to deliver data to the outside world. E.g. A smart lock that would unlock the door after the payment is received.
- Consensus-based Oracles: They get the data from human consensus and prediction markets.

In this work, reference will be made to a hardware oracle, since they are directly related to IoT devices, although the fundamental aspects regarding decentralization are valid for any type of Oracle.

4.6 Oracles: A point of failure

In a blockchain network, the devices responsible for entering information are called Oracles. An oracle could be for example temperature, humidity, or any other sensor that enters data into the blockchain.

Single IoT devices are exposed to the same problem that smart contracts themselves seek to avoid, a single point of failure. The reliability of the information depends completely on the information provided by the Oracle. The information that is entered in a blockchain created for an IoT network will depend on the devices that compose it. Because the devices are physically vulnerable to attacks or manipulations, such information could be compromised even before entering the blockchain and therefore being already entered with erroneous information. The problem is then that smart contracts cannot access data on their own the data must rely on an oracle which could be tampered. Usually, oracles have centralized structures, and consequently, are susceptible to the problem of a single point of failure. If an attacker manages to manipulate the information of the central axis that maintains the structure of the oracles, he can manipulate the information of these. For example, if a decentralized platform that works on blockchain uses a single oracle as a source of information and

this oracle is attacked, the information that enters the decentralized platform will be incorrect, triggering a series of problems. Such is the case of the attack on the bZx platform (74), a platform that allows obtaining credit by leaving a collateral, used as a source of information on the dollar, a single oracle. This being manipulated and momentarily increasing the value of the dollar, allowed the attacker to manipulate the loans granted and take an equivalent in cryptocurrencies of 630,000 USD at the time of the attack.

To avoid the above, it is also necessary to decentralize the architecture of the oracles, to ensure that the attack on an oracle does not affect the rest of the network. By allowing multiple oracles through a decentralized network to evaluate the same data it is possible to erase any one point of failure, maintaining the value of smart contracts, and keeping the information secure, reliable and trustworthy. Chainlink, a case study explained in *Chapter 6*, proposes to verify the accuracy of the data provided with individual oracles with others, helping to guarantee the correct trigger of the smart contract.

5 Solutions

In this chapter, the different ways that a blockchain has of developing solutions to the challenges that arise over time such as scalability (in terms of the number of transactions per second), connectivity, interoperability, and energy efficiency are introduced. These solutions can be classified into four types of on-chain solutions, off-chain solutions, consensus mechanisms or the use of other forms of distributed ledger (e.g. Directed Acyclic Graph).

The following image groups solutions developed in the field of scalability in classified projects according to the aforementioned classification.

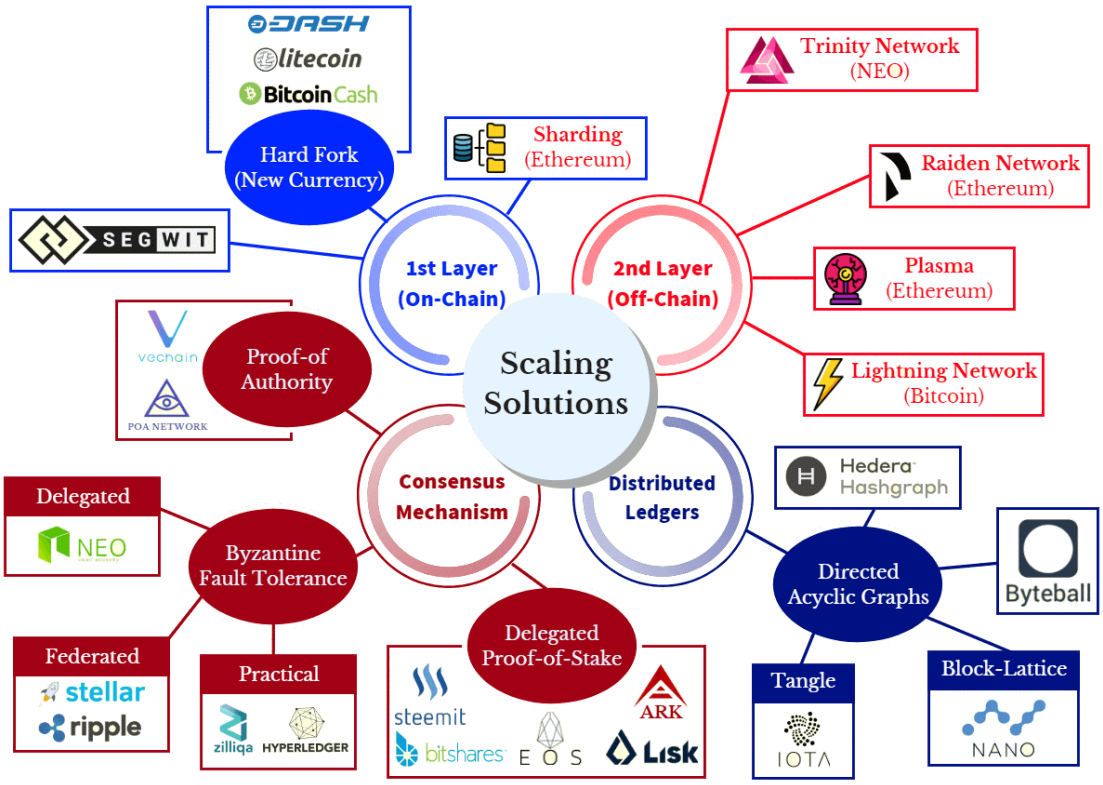


Figure 5-1 DLT-based networks scaling solutions (75)

The characteristics of each solution are detailed below:

- **First layer solutions:** also called protocol-layer solution or on-chain solutions are fundamental changes that are carried on the current blockchain to improve scalability. As mentioned before, in this category are the options of increasing the block size or reduce the creation time of the blocks. In the on-chain, a transaction is validated by modifying the blockchain (being added to the blockchain), that is why it has to wait to be confirmed by all of the nodes on the block.
- **Second layer solutions:** also called off-chain solutions, imply the use of other blockchains as side chains to improve scalability. The sidechains are alternative blockchains pegged to the main blockchain which provide expansion capabilities carrying the bulk of transactions of the mainnet[34] to reduce congestion. However, using a side chain make major security tradeoff compared to transactions done in the mainnet only because the security remains also in the second layer used. Off-chain transactions provide easy access between blockchains enabling cross-chain transfers. Off-chain transactions validate the transaction through multiple methods of getting records of the immediate transaction and immediately ensuring that it won't be reversed, being able to reduce the waiting time for

[34] A mainnet is a blockchain that performs the functionality of transferring a digital currency from a sender to a recipient. Mainnet is simply the main network, whereby actual transactions take place on a distributed ledger.

confirmation. Examples: Plasma for Ethereum blockchain, Lightning network for Bitcoin blockchain.

- **Consensus Mechanisms:** the consensus mechanism of the blockchain is the one that allows, coordinates, and decides how the scalability of the blockchain will be carried out and how it will evolve over time. Without an appropriate consensus algorithm, the network could have difficulties adapting to the new market needs (as is the case with Bitcoin).
- **Scalable distributed ledgers:** they represent an alternative to blockchains using a different structure to organize transactions or data. IOTA case study, which is going to be explained later, is an example of a different ledger structure, it uses Tangle that is a directed acyclic graph (DAG)

5.1 First layer solutions

As an example, the concept of sharding in the blockchain is explained, which is a first layer type solution mechanism for scalability. Sharding is often referred to as a first layer solution because it is implemented at the base-level protocol of the blockchain. It is a concept widely used in databases. It is a type of database partitioning that separates large databases into smaller parts called shards, which are faster and more easily managed. This spreads the load and improves efficiency. In the blockchain, each node instead of having the full information of it will have only a part of the data. The information contained in a shard can still be shared among other nodes, that way, the ledger is still decentralized and secure because everyone can still see all the ledger entries. Sharding is one of the most promising scalability solutions for blockchain networks. However, this solution does not apply to the PoW consensus algorithm (since the nodes need to have the information of the whole blockchain) but to Proof of stake one.

However, some issues with this method can still be found. Without downloading and validating the entire history of a particular shard the participant cannot necessarily be certain that the state with which they interact is the result of some valid sequence of blocks and that such sequence of blocks is indeed the canonical chain in the shard (76).

5.2 Second layer solutions

Sidechains are often referred to as second layer solutions and are the result of multiple blockchains, which exist separately but are linked to the root chain (original main chain) and a third cross-chain solution (77). The second layer solutions use other parallel chains that fulfill the function of assisting and complementing the main blockchain in the tasks that are required. For example, they can be used to increase transaction speed, network security, provide another consensus mechanism, increase

energy efficiency, among others. The use of sidechains allows the main network to generate solutions to the problems that arise over time without having to make major changes in the main blockchain since the development of the solution is carried out in another chain of blocks that will work in parallel. Among examples of developed sidechains it can be mentioned Plasma project (for Ethereum blockchain), Liquid and Lightning network (for Bitcoin blockchain), POA (for Ethereum blockchain), among others.

5.3 Consensus mechanisms for IoT

To achieve the creation of a decentralized IoT network, that is, without the need for a controller or a central data storage source such as the cloud, different IoT devices (usually referred to as "nodes"), must interact with each other in a P2P manner. This communication paradigm solves the problem of a single point of failure. However, in order to carry out a correct communication and decide on the information that will be validated, a consensus mechanism is necessary that allows all the walls to make the decisions without the need of a central authority (78).

Despite the original integrated mechanism that ensures data integrity in blockchain-based systems (Proof of work), its implementation in IoT networks with limited resources is a challenge and not feasible for the following reasons:

- The calculation of cryptographic hashes in the context of the consensus method requires many calculations not necessarily achievable by low-powered devices.
- As the network grows, communication between nodes requires a greater number of interconnections, so without a proper mechanism, the consensus mechanism can become inefficient and even more in limited spaces where IoT devices could interfere with them.
- IoT networks are made up of many devices that need to communicate with each other. When that communication has to be made quickly and in every moment the need for low latency consensus methods is a challenge to overcome (since in PoW consensus, the higher the time to reach consensus, the higher the security).

It is important to highlight the limitation that many IoT devices use batteries for their operation, so maintaining high energy efficiency in the network is essential. P2P communications networks require devices that are constantly providing information to the network and, consequently, have been connected to it, therefore constant energy consumption. As one alternative of consensus mechanisms, Proof of Stake (PoS) has been proposed as a cleaner option to PoW (79).

There are many consensus mechanisms currently developed, but many of them are not promising for an IoT network (for example Proof of Capacity, Proof of Activity, Proof

of Burn) (27) in this section, the friendliest DLT consensus alternatives for an IoT network will be discussed.

Proof of authority: The Authority Test is designed to be a practical and efficient solution, especially aimed at private blockchains. Similarly to the Proof-of-Work based networks, Proof-of-Authority (PoA) blockchains consider transaction validation as a job that should be rewarded and encouraged. PoA takes advantage of real identities to allow validation within a blockchain. This means that the nodes put their real identity and reputation as a guarantee of transparency. However, a process that includes an arbitrary selection of such reliable validators, so its use would be limited to private blockchains, where nodes are chosen and decided to act as validators. This consensus mechanism is also known for delivering faster transactions and being more efficient than other protocols since communication between nodes is not necessary to reach a consensus. Scalability is also a great benefit because of this, making it an attractive option for business-scale projects.

Besides, PoA is based on a limited number of validators. This feature gives it a clear advantage, the high scalability of the blockchain. What has a positive impact on applications where speed is paramount

Proof of authentication (PoAh): It is a consensus mechanism developed by D.Puthal & S. Mohanty (80) and specially designed for the lightweight implementation of blockchains in the Internet of Things (IoT). PoAh consensus mechanism follows a traditional blockchain working model, that is, a blockchain where each block contains a hash of its own attached to the hash of the previous block. The difference with PoW is that the block verification is made through lightweight computational power. Trusted nodes are in charge of the authentication process of the blocks to be added to the chain. The authentication process considers two steps:

1. Authenticate the block and source of the block.
2. Upon validating the authenticated block by trusted nodes, increase the trust value by one unit for those who have authenticated the block first.

Miners who perform false authentications lose a unit of trust value and becomes a normal node in the network after a certain number of false authentications. That way, only nodes with good behavior over time remains as validators.

Practical Byzantine Fault Tolerance (pBFT): This consensus mechanism was already explained in *Chapter 1* so that its benefits and disadvantages will be explained here. The benefits of the PBFT consensus algorithm:

- Highly scalability and low transaction fees: pBFT is highly scalable as long as the number of participating nodes is not high. So, its operation in private blockchain networks is ideal to achieve high transaction rates per second.

- Energy reduction: the model offers a good reduction in energy consumption compared to PoW.
- Transaction finality: The nature of pBFT means that transactions can be agreed upon and finalized without needing multiple confirmations. There is no waiting period to ensure a transaction is secure after including it in a block.

pBFT disadvantages:

- When using a reduced number of nodes, is susceptible to Sybil attacks, where a single party creates or manipulates a large number of nodes in the network and compromises security.
- Scalability is high only if a limited number of nodes is maintained, so it is not possible to have a highly decentralized node system.

5.4 DLT alternatives for IoT

The alternatives of distributed ledger technology are alternatives to the blockchain that have a different architecture. In this case, an example (called Tangle) of Directed Acyclic Graph (DAG), that is used in IOTA, will be discussed, the case study presented in the last chapter.

Tangle: the consensus mechanism in the tangle does not work like a linear blockchain, it is a different type of DLT. The architecture is not based on a chain of joined blocks but in sidechains. A sidechain allows different transactions to be carried out independently in multiple chains and at the same time, reducing the creation and validation time of a block. In a blockchain, the transaction is confirmed after it is approved by several blocks. Similarly, when the transaction has enough cumulative weight (it has been validated by different nodes over time performing PoW) it is safely included in the consensus. The consensus mechanism uses a small calculation of PoW but operates under rules and in a different architecture (16). This system will be analyzed in greater depth in *Chapter 7* when the case study is presented, but it is anticipated that it is a highly scalable consensus mechanism designed to work in IoT devices.

5.5 Interoperability

In the traditional business sector, the problem of isolated data and its negative impact on the efficiency of the process has been a strong point for decades and still is. The interoperability problem must be developed to exploit the potential of blockchain technology, as indicated by the European Union Blockchain Observatory and Forum (EU Blockchain), which mentions the need to generate a high level of interoperability between blockchains as well as introducing the first standards for it (81).

At the interoperability level, there are solutions that are being developed at different scales to achieve compatibility between different blockchains.

Cross-platform blockchain: at a global level, Cosmos cross-platform blockchain project tries to solve the compatibility problem between blockchains generating a macro-solution. Basically, this blockchain works as an intermediary blockchain to allow communication between two other main blockchain types such as the Ethereum blockchain and the Bitcoin blockchain. Cosmos Hub, an initiative of the Cosmos project, acts as a coordinated blockchain that forms a bridge between different channels, allowing each to detect the status of the other and to exchange assets without trust between the networks. In addition to allowing existing block strings to connect, Cosmos provides a network of individual public channel chains with which developers can interact. Each blockchain (called "Zone" in Cosmos terminology) is built on the same standard protocol and can be seamlessly connected to the bridge blockchain, called the cosmos hub (82).

In addition to cosmos, Clearmatics (83) and Chainlink (15) propose cross-chain technology in smart contracts, there are some other initiatives between platforms to generate interoperability such as AION, ICON, and Wanchain (84) (85), which together form the Blockchain Interoperability Alliance and are working on their own multilevel blockchain networks that involve some degree of interoperability. The NEO and ONT blockchain protocols also created an interoperability initiative creating a partnership to build an open cross-chain platform (86).

Most of the information found were only research concepts or proposals to be developed, therefore, it should be mentioned that developments in the field of interoperability are still scarce for a large number of blockchains that are being developed and that at the moment the efforts are put into generating blockchains that outperform the rest that generate compatibility. However, as in the beginning, it happened with cell phones, where each one generated its own operating system, it is possible that in the future the tendency is to interconnect blockchains to generate a more complete ecosystem.

6 Case study - Chainlink

Mentioned the previous problem and the disadvantages and vulnerabilities of trusting a centralized system as a source of information for the blockchain, a case study will be introduced in this section, a company that is developing a solution in this regard: Chainlink, a decentralized oracle network.

Why an ideal Oracle is hard to achieve

There is no perfect data source from where obtain information or service provider unconditionally trustworthily. Data could be intentionally or not corrupted. What differentiates Chainlink from other oracle solutions is its ability to operate as a fully

decentralized network. This decentralized approach limits the trust in any single party, enabling the tamperproof quality valued in smart contracts to be extended to the end-to-end operation between smart contracts and the APIs they rely on. The information presented below is explained in a summary way to highlight the potential of the project for the decentralization of information from oracles. The detailed functioning can be found in detail in (15). The main objective of the company is to safeguard the benefits of the blockchain (decentralization, security, and immutability) in the information that is ready to enter the blockchain. In this way, it is achieved that the information cannot be altered before entering the blockchain and can, consequently, be a reliable source of information.

Architectural overview

The architecture is composed in two parts, on the one hand, there is the one on-chain architecture where the oracles adhere to the decentralized Chainlink network and on the other the off-chain architecture where oracles are connected directly to the Ethereum network. Chainlink has been built originally in the Ethereum network, but it is intended to support off-chain and cross-chain interactions for leading smart contracts networks. The core functional objective is to link on-chain and off-chain environments.

On-chain architecture

In this environment, Chainlink returns replies to a data request made by a user smart-contract (called User-SC). Chainlink itself acts with an on-chain smart contract (called Chainlink-SC) that is responsible for responding to solicitudes. In addition to that smart-contract Chainlink works with three other Smart contracts that help build trust and credibility in the oracles that provide information to the blockchain as well as discard oracles that have inadequate co-behavior:

- Reputation contract: it is in charge of the performance metrics overtime of the oracle service provider.
- Order-matching contract: it receives the proposed service level agreement (SLA) from the user, logs the parameters, and collects bids from the oracle providers. Providers with higher reputation levels are taken into consideration.
- Aggregating contract: It collects the oracle providers' data returns a collective result, providing also the data of the oracle provider to the reputation contract.

The on-chain workflow process works as follows:

Oracle selection→ Data reporting → Result aggregation on the blockchain

The oracle service purchaser specifies the service level agreement (SLA) that wants to apply (example later in *section 6.3).* In the SLA it is possible to find aspects such as query parameters and the number of oracles that the purchaser wants to request

information from. In this step, the purchaser gives also the parameters for the reputation and aggregation contract. When manual contract selection is not possible, Chainlink also has automatic contract matching, useful in situations when the request of the oracle is done dynamically in response to the load of the smart contract.

Off-chain architecture

As mentioned before, Chainlink works currently with the Ethereum network but is intended to be compatible with the main blockchains. Oracles nodes from Chainlink, running in ETH blockchain and in a decentralized manner, harvest responses to the off-chain requests. This data is aggregated via any possible consensus mechanisms into a global answer to the User-SC.

Oracle security

As explained before, a well-functioning blockchain has the advantages of being secure, immutable, and decentralized, preventing the information from being tampered. The threat to security is however if the information written in the blockchain is reliable. Oracles, which provide the information to the smart contracts of the blockchain, need to be highly trustworthy to preserve the reliability of the information. The security of a whole system depends on the weaker point of it.

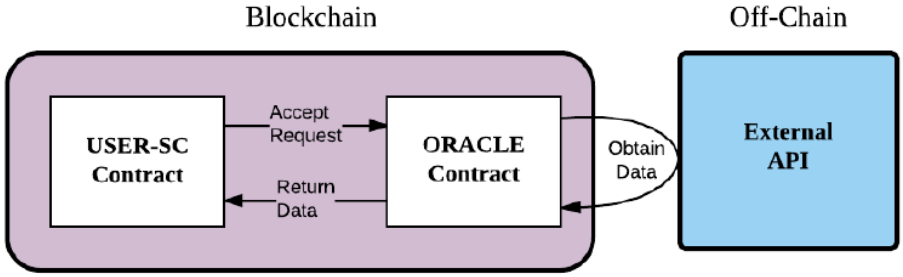


Figure 6-1 The behavior of an ideal oracle

Chainlink decentralization approach

Three basic complementary approaches to ensuring against faulty nodes are proposed, where the first two involve the decentralization of the data sources and oracles.

- **Distribution of data sources:** in the mentioned solution, data of the oracle is obtained by multiple sources, which is in turn added to an aggregate function[35]. If some source throws some data out of range could be considered an outlier and not taken into account. In turn, if most resources return an identical value, the entire function will yield that result. Otherwise, it returns an error.
- **Distribution of oracles:** just as the sources of data can be distributed, Oracles can have a distributed approach. Instead of a single oracle node O, there may be a group of n different oracles $\{O_1, O_2, \ldots, O_n\}$, where each oracle O_i has a

[35] An aggregate function or aggregation function is a function where the values of multiple rows are grouped together to form a single summary value

distributed data source system, which can overlap or not with the other distributed data sources.

- **Use of trusted hardware:** For the entire ecosystem to function, physical oracles must come from reputable suppliers to avoid prior manipulation via hardware.

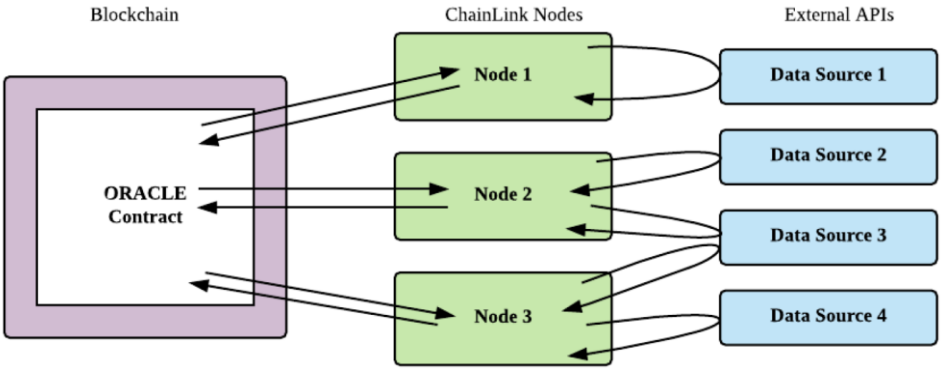


Figure 6-2 Two-level distribution scenario

6.1 Freeloading problem

A problem that arises with the decentralization of oracles is the so-called "freeloading". A cheater oracle could avoid the energy costs and expenses of obtaining the data for it and copying the data provided by another oracle. This problem declines the distribution of the data sources as well as the rapid response of each one (responding slowly and freeloading is a cheaper strategy), so that the response of an oracle that copies the response of another, would be delivered later than the original. To avoid this, Chainlink a random request for data with its smart contract, first collecting the data before being disclosed (normally the data is revealed before being collected by the smart contract), thus excluding potential freeloaders in said data collection

6.2 Off-chain aggregation phase

This phase represents a medium-term solution. The first stage of decentralization, although it potentially solves the security of the information that enters the blockchain, has a disadvantage of efficiency, the cost of transmitting all that information in the main blockchain (on-chain contracts) is high, this will happen while in the Ethereum network (the one initially used by Chainlink) maintains a structure of PoW, which materializes the cost of the transfer of said information in the form of fees (gas[36] in the case of Ethereum).

[36] Ethereum Gas is a unit that measures the amount of computational effort that it will take to execute certain operations and is used to pay for these operations. This will happen while maintaining a PoW structure, although in the future the network plans to change its consensus mechanism to a proof of stake, where it would no longer be necessary to pay for transactions, possibly eliminating the use of gas.

The solution to the above problem is to concentrate much of the information coming from the oracles to an off-chain blockchain, and subsequently send a unified response to the smart contract (Chainlink-sc) to the main network. However, with this solution, again the problem of freeloading appears because when using an external blockchain, a consensus mechanism is relied on other than that of Chainlink, so the solution stated in the first point is no longer feasible and will depend on the provider execute a timely mechanism to avoid the problem. The proposed solution to this matter is much more technical and will not be fully exposed in this research work, it involves the use of Schnorr signature[37] (87) and an OCA[38] protocol composed of two pairs of algorithms carried out by the participating oracles and those executed by the provider (which could be a smart contract external to the main blockchain). The OCA protocol also involves the use of incentives for nodes that have good behavior over time. This would allow finding and isolating possible faulty nodes as well as rewarding good behavior to nodes that provide reliable information over time.

6.3 Operation Example

Below is a working use case of Chainlink with China's blockchain-based service network (BSN). BSN is a blockchain infrastructure service layer designed to be a one-stop-shop for companies to access ultra-low-cost blockchain cloud computing services. It's supported by major Chinese entities and corporations, and its founding consortia partners include China's State Information Center, China Mobile, China Unionpay, and Red Date Technologies. For the moment China's BSN is integrated with six public blockchains, that will open its services to decentralized applications (dapp) developers.

BSN selected Chainlink as the preferred oracle network to enable BSN applications and smart contracts to access data from outside the blockchain, also called off-chain data (e.g. weather, financial asset prices, IoT data, location information, and much more) (88).

The operation process is detailed below:

1. Smart Contract on BSN triggers use of any off-chain API, from any blockchain connected to IRITA.[39]
2. Data request forwards to the service Hub through an inter-blockchain communication protocol.

[37] The Schnorr authentication protocol is a zero-disclosure proof of knowledge described in 1989 by Schnorr, whose security is based on the difficulty of the discrete logarithm problem and used to prove the knowledge of a discrete logarithm.

[38] The Open Control Architecture (**OCA**) is a communications **protocol** architecture for control, monitoring, and connection management of networked audio and video devices.

[39] IRITA is a consortium blockchain product that provides an interchain service hub for next-generation distributed applications.

3. Chainlink uses several data sources to satisfy the data requirement and places the off-chain API's data back on-chain for use by the smart contract.
4. Off-chain data is forwarded back to the BSN based smart contract that initiated the request.

The following image shows the part in which Chainlink is involved.

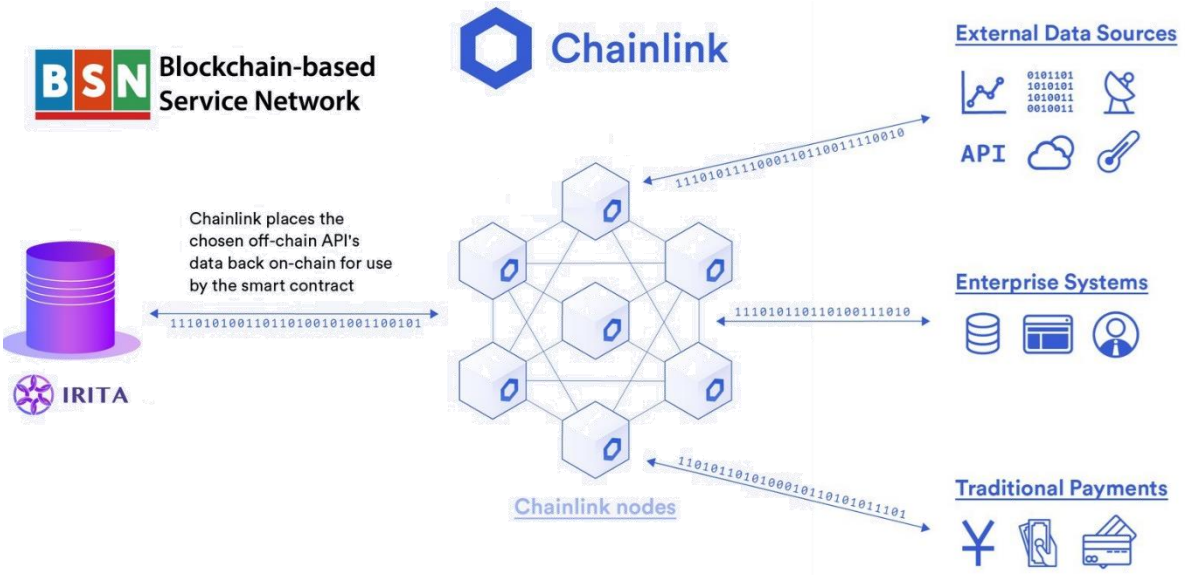


Figure 6-1 Chainlink as an oracle provider in the blockchain-based service network

6.4 Conclusion of the case study

The decentralization work of the nodes or IoT devices that provide information to the blockchain is an initial and pioneering step of Chainlink. The company aims to be the first provider of a decentralized oracle system for Ethereum and other blockchains and has taken an initial step and has been collaborating in the development of a network of decentralized oracles with companies such as Google (89), SWIFT (90), Gartner (91) and the Cornell University with its program IC3 (92). Also, its recent integration with China's recently launched national Blockchain Services Network (BSN) positions Chainlink as a leader in the oracle decentralization industry. This key integration will enable governments and enterprises to incorporate validated real-world data into their BSN applications using Chainlink oracles via the IRITA interchain service hub (88). It should be noted that the decentralization of oracles represents a great challenge to achieve information stored in the blockchain that is trusted, reliable and tamper-proof, which are precisely the benefits of a blockchain network but are not characteristics in a current network of IoT devices that provide data. The company proposes initial and medium-term solutions to achieve such decentralization and overcome the incentives to manipulate information, however, they keep in mind that research work and solutions to prevent fraud must be constant since the ways of attempted manipulation evolve over time.

7 Case Study - IOTA

As proposed by T. Fernandez and P. Fraga (22), traditional databases or Directed Acyclic Graph (DAG) based ledgers may be a better alternative than blockchains for certain IoT applications. IOTA with its DAG called Tangle (16), is presented in this section.

IOTA is an open-source distributed ledger technology, which aims to safely allow the exchange of information and value on the Internet of Things. One of the main innovations of IOTA is that, instead of the traditional blockchain, it uses its own architecture (Tangle) based on a mathematical concept called the Directed Acyclic Graph (DAG). This architecture makes it possible that there are no commissions, low network latency and better prospects for scalability. IOTA aims to eliminate the need for blocks and allow better scalability. Each creator of a transaction on the network has to approve two previous transactions through computational work (PoW). Thus, the process in which transactions are made is done without commissions as a reward for helping to protect the network. Thanks to the fact that there are no transaction fees, microtransactions (small-value transactions) can be made.

7.1 Tangle's architecture

IOTA's architecture is based on a DAG which they call Tangle. Being based on a DAG allows IOTA to be very well directed towards scalability but that in turn makes it somewhat complex. Its consensus mechanism is based on verifying two transactions and has no transaction fees beyond this. The operation of the tangle is explained in detail below. Unlike the blockchain, where the information is coupled in blocks one after another, in the DAGs the information is stored in parallel, forming a network.

In the following Figure, green squares are transactions already confirmed by the network with a certain grade of certainty, grey squares represent unconfirmed transactions, therefore, without any validation (Tips), blue squares have been partially confirmed but still, there is uncertainty due to the lack of more subsequent confirmations.

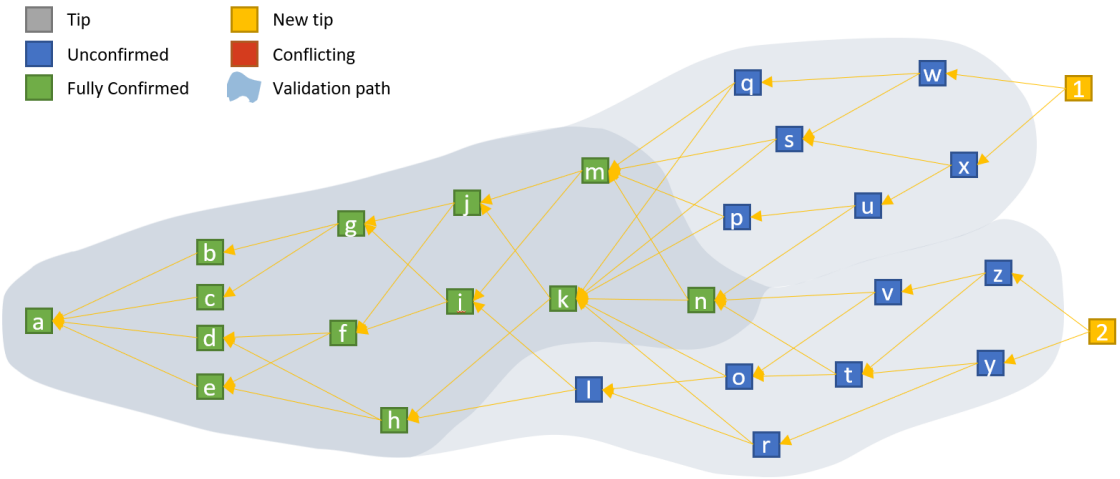


Figure 7-1 Representation of the Tangle

Each square of this scheme represents a transaction in Tangle, in addition, each square point to two others. The arrows represent the act of approval of a transaction, and each transaction needs confirmation of two other future transactions to be partially validated. In order to create a transaction (Tip), a user needs to validate two previous transactions from other participants in the network. For example, in the previous illustration, the new transaction "1" is directly validating the transactions "w" and "x", while it is indirectly validating the transactions prior to these ("q", "s", "u", "p", etc.). At the same time, another new transaction "2" does the same with "z", "y", "v", "t", etc. With this structure, it is achieved that, as new transactions validate the previous ones, a constant and indirect validation is generated in the time that confirms with increasing certainty that the transaction is valid. It can be noticed that the group and the squares in green, has been indirectly confirmed by Tips "1" and "2", so they have been validated by many other transactions and, therefore, are considered fully confirmed transactions. On the other hand, the upper blue transaction group has only been indirectly validated by Tip "1" so they must wait to be indirectly confirmed by other Tips simultaneously to be considered fully confirmed (16).

As more Tips are added to the network and indirectly validated, a series of weighted validations is generated that is represented in *Figure 7-2* with the dark areas. The darker the area, the more indirect validation it has had, so the greater its degree of confirmation.

In the case where two fraudulent transactions are added as shown in the *Figure 7-2* figure with "w" and "y" the subsequent tips ("1", "4", "2") will not be aware of the manipulation since they are not validating both transactions indirectly at the same time.

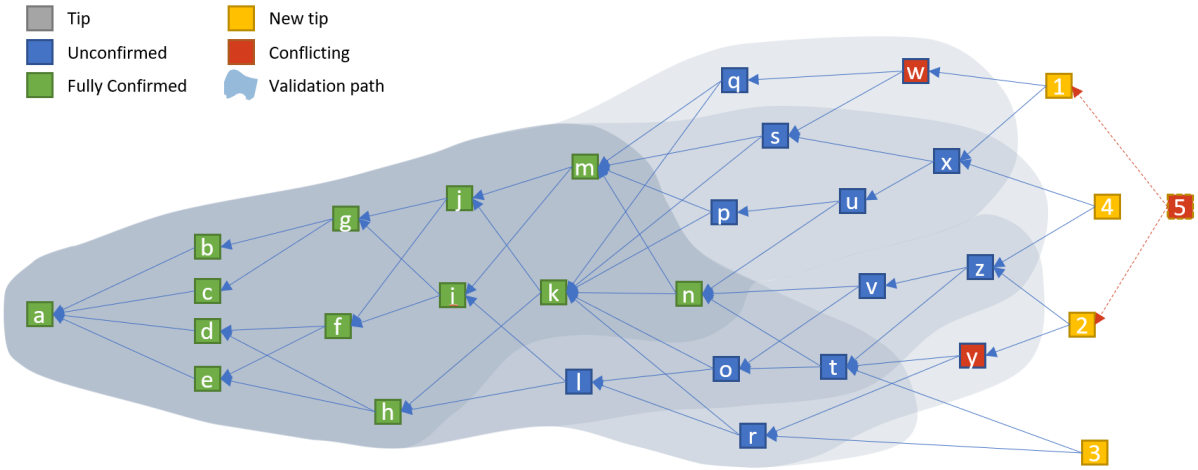


Figure 7-2 Tangle with conflicting transactions present

However, over time, Tip "5" is added and it is assigned to validate the previous Tips "1" and "2", and seeing at the same time that "w" and "y" do not have a correct match about the previous transactions, it discards the fraudulent Tips and look for new ones to validate. This way, fraudulent transactions will never be confirmed a number of times high enough to be considered completely valid.

7.2 Strengths

The following briefly indicates the strengths that the IOTa proposal presents to generate a payment network and information processing of integral IoT devices:

- **Transaction rates:** one of the biggest issues with the blockchain, as originally developed for Bitcoin, is its slow transaction times and in some cases, expensive ones. Given the structure of IOTa, the more users connect to the network and carry out transactions, the greater the speed of the confirmations and the lower the latency involved, so the greatest strength of the architecture is that it becomes more efficient in time response as the network grows (16).
- **Micro-Payments:** in the IOTA's Tangle, microtransactions between devices are much easier and more cost-efficient. This offers a new range of opportunities for companies since the handicap of high commissions will no longer be present.
- **Scalability:** from a purely technical standpoint, IOTA's tangle has, in theory, no limits as far as network-growth is concerned. Since in order to carry out a transaction, two previous transactions must be validated, a greater number of transactions added to the network do not represent an unsustainable increase in the use of processing power.
- **Masked Authenticated Messaging (MAM):** it is a feature that gives the possibility to the nodes to exchange data through Tangle in a totally encrypted and authenticated way. This means that all intelligent devices can transmit data of maximum sensitivity without the possibility of being tracked. For example, a

channel can be created where several people can share confidential information without any fear that it can be "heard" by other people or devices.

7.3 The centralized coordinator problem

The architecture presented by tangle is presented as an alternative with great potential to solve the scalability problems that most blockchains possess. In blockchains that use the PoW consensus mechanism, the verification of the blocks increases their reliability the greater the computational processing power that supports it through the PoW. On the other hand, in the Tangle, the PoW mechanism is only used in small quantities and the reliability of the transaction increases with time and the number of verifications instead of the brute force of the capacity in a given instant of time.

In a blockchain, each block is accepted or not by the consensus of the nodes. In the Tangle, even though in theory it can work without problems, in practice a central coordinator is currently required to provide security to the network in its initial stages given the danger of malicious actors. For example, if corrupt transactions were assigned to other Tips simultaneously and indefinitely, the Tangle would grow with transactions that were corrupt since its inception. That is why the central coordinator, in charge of selecting the transactions to be validated, is currently controlled by the IOTA foundation.

However, as explained above, the strengths of the distributed ledger technology are that it be as decentralized as possible in all its aspects to increase the overall security of the system so that a central controller is susceptible to external attacks given its centralized nature. It is due to the above, and in the search for the total decentralization of the system, that IOTA proposes the use of The Coordicide, a decentralized coordinator, who will be responsible in the future of assigning the transactions to be validated in a completely autonomous and decentralized manner. At the time of this research work, The Coordicide (93) is a concept in development that is currently implemented and being tested, but which raises the basis for a DLT with all the potential to host a network of IoT devices with scalability, in theory, without limits and providing the same benefits that a blockchain grants. The detailed explanation is beyond the scope of this work, but at a general level the decentralized coordinator vision involves several modular solutions. Among them, there is a voting scheme between peers, where by means of a probabilistic consensus mechanism they simultaneously consult the status of the ledger. The second aspect is the reputation of the nodes, associated with their identity. Those nodes with the highest number of transactions on the network over time will have a higher reputation.

In addition to the implementation of the decentralized coordinator that represents one of the main challenges, there are other aspects that IOTA must improve to present itself in the future as the undisputed alternative for an Internet of Things environment:

- **Energy consumption:** the current challenge to IOTA is that transaction signing operations are still computationally complex relative to the limited capabilities of many IoT devices and may be impractical on energy-limited/battery-powered devices.
- **Reaction times (latency):** even when the response times are incredible compared to many blockchains, to position themselves as an option for the entire spectrum of IoT devices, the reaction times must be negligible. IOTA has problems in light devices (lighter than a raspberry Pi), taking up to 100s its PoW and up to 1s its signature. Therefore, for cases where transactions of microseconds or very limited response times are required, optimization is still necessary since those times are only achievable with devices that can contribute with greater computational power to reduce those latency times.

7.4 Conclusion of the case study

Even though the mathematical concept of directed acyclic graph, is much older than the creation of the first blockchain, it is the inclusion of the PoW method as a consensus mechanism, together with the approach made for IoT devices and a decentralized coordinator that gives IOTA the potential of being a network protocol capable of supporting the Internet of Things networks of tomorrow. In the traditional centralized financial system PayPal can handle an average of 193 transactions per second, and Visa can handle 1667 transactions per second while the IOTA mainnet in its current stage 1.5, can handle 1000 transactions per seconds, and this number is expected to grow in the future (94). Although not mentioned in the case study, IOTA has a large number of partnerships with companies such as BOSCH, Fujitsu, IBM, Nokia, Orange, Oracle Corporation, Porsche AG, Vodafone Group, Volkswagen AG, among others as well as many reputable universities around the world (95), what makes it the most promising DLT project today in the field of Internet of Things.

8 Conclusion

This research work focused on the potential of the integration of blockchain technology to strengthen networks of IoT devices, providing essential aspects to maintain a network according to the requirements of the current industry such as reliability and security in the transmitted data.

Even though blockchain technology was originally conceived as a decentralized payment network, with the passing of time and the development of technology, several additional uses have emerged, such as the inclusion of smart contracts and the development of another consensus mechanism. The current developments in the blockchain open the possibility to develop new business markets as well as improve current ones in aspects such as smart-health, smart cities, traceability in the supply

chain, insurance industry, automated payments, among others. Many of these markets, whether they are industrial or not, involve the use of the Internet of Things devices. In addition, much of the data collection and transmission is carried out through these devices and explains the exponential growth that IoT device networks have experienced in the last time. It is in the growing Internet of Things market that blockchain has all the potential to be an essential complement in the future. If current developments are completed and the challenges mentioned are overcome, blockchain could maintain a secure and reliable IoT network through the decentralization of all or at least part of the system's architecture. Although there is currently no sufficiently advanced development of blockchain to be applied efficiently in an IoT network, the solutions to the challenges involved are under development, and it is expected that over the years, these solutions will be successfully implemented in the IoT networks.

It is also concluded that other projects that have been born thanks to the development of the blockchain, and that are developed in an external environment such as Chainlink and IOTA are pioneering projects in their areas and at the moment, those that have the greatest potential for success. In the case of Chainlink, although it is in the early stages of development, they are the first who raised the concept of decentralizing the information before it enters the blockchain. Decentralizing and increasing data security in the sources from which the information originates has an enormous potential of development and that is why the project is supported by recognized companies and organizations worldwide. In the case of IOTA, they are currently the DLT project with the greatest scope in the industry in terms of partnerships as well as development potential regarding the IoT scope. If the company is able to implement the decentralized coordinator in its network, it would represent a definitive step to guarantee security and reliability to IoT networks in a decentralized manner and with unlimited scalability.

With the invention of the telephone and later the digital revolution and the development of the internet, the world has experienced the connection between people. In the society of the future, the total interconnection of things will be a reality, and the structure capable of supporting all the flow of data and also being able to guarantee security and reliability in the information is being developed at the moment.

9 Bibliography

1. *A Blockchain Research Framework.* **Risius, Marten and Spohrer, Kai.** 2017, Business & Information Systems Engineering, Vol. 59, pp. 385-409.

2. *Bitcoin: A peer-to-peer electronic cash system.* **Nakamoto, Satoshi.** 2008.

3. *Internet of Things.* **Ashton, Kevin.** 2009, RFID journal, pp. 97-114.

4. *IoT Challenges.* **Kranenburg, Rob Van and Bassi, Alex.** Gent : SpringerLink, August 13, 2012, SpringerOpen Journal, pp. 1-5.

5. **Reyna, Ana, et al.** On Blockchain and its integration with IoT. CHallenges and opportunities. *Future Generation Computer Systems.* May 24, 2018, pp. 173-190.

6. *Internet of Things: Security Vulnerabilities and Challenges.* **Ioannis, Andrea, Chrysostomou, Chrysostomos and Hadjichristofi, George.** Larnaca : s.n., July 6, 2015, IEEE ISCC 2015 International Workshop on Smart City and Ubiquitous Computing Applications, pp. 1-8.

7. *Management of resource constrained devices in the internet of things.* **Sehgal, Anuj, et al.** 12, s.l. : IEEE, December 2012, IEEE Communications Magazine, Vol. 50.

8. *Blockchain for IoT security and privacy: The case study of a smart home.* **Dorri, Ali, et al.** Kona : IEEE, 2017. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).

9. *Blockchain Platform for Industrial.* **Bahga, Arshdeep and K. Madisetti, Vijay.** 2016, Scientific Research Publishing.

10. **Saptarshi, Gan.** *An IoT simulator in NS3 and akey-based authenticationarchitecture for IoT devices usingblockchain.* Indian Institute Of Technology Kanpur. 2017.

11. *Can Blockchain Strengthen the Internet of Things?* **Kshetri, Nir.** 4, s.l. : IEEE, August 17, 2017, IT professional, Vol. 19, pp. 68-72.

12. *Governance in the Blockchain Economy: A Framework and Research Agenda.* **Beck, Roman, Müller-Bloch, Cristoph and King, John Leslie.** Atlanta : s.n., June 9, 2017, The Journal of The Association for Information Systems, pp. 1-15.

13. *A blockchain future to Internet of Things security: A position paper.* **Banerjee, Mandrita, Lee, Junghee and Raymond Choo, Kim-Kwang.** 2017, Digital Communications and Networks.

14. **Circle Research.** *Vodafone IoT Barometer 2017/18.* s.l. : Vodafone Group, 2017.

15. *Chainlink, a Decentralized Oracle Network.* **Ellis, Steve, Juels, Ari and Nazarov, Sergey.** september 4, 2017, [Study Topic]. Unpublished raw data, p. 1.

16. *The Tangle.* **Popov, Serguei.** April 30, 2018.

17. *Pervasive Decentralisation of Digital Infraestructures: A framework for Blockchain enables System and Use Case Analysis.* **Glaser, Florian.** 2017. Proceedings of the 50th Hawaii International Conference on System Sciences.

18. **Zhegu, Majlinda and Olleros, Xavier.** *Research Handook on Digital Transformations.* Cheltenham : Edward Elgar, 2016.

19. *Rethinking Permissioned Blockchains.* **Vukolic, Marko.** Zurich : IBM Research, April 02, 2017, Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, pp. 3-7.

20. *Hyperledger fabric: a distributed operating system for permissioned blockchains.* **Androulaki, Elli, et al.** Porto : s.n., April 23, 2018, EuroSys '18 Proceedings of the Thirteenth EuroSys Conference.

21. **Baliga, Arati.** *Understanding Blockchain Consensus Models.* Persistent. Bhageerath : s.n., 2017. pp. 1-14.

22. *A Review on the Use of Blockchain for the Internet of Things.* **Fernández-Caramés, Tiago M. and Fraga Lamas, Paula.** Coruña : s.n., May 31, 2018, Department of Computer Engineering, University of Coruña.

23. *An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends.* **Zheng, Zibing, et al.** Honolulu : s.n., June 25, 2017, 2017 IEEE 6th International Congress on Big Data.

24. **Buterin, Vitalik.** Medium. *The Meaning of Decentralization.* [Online] february 6, 2017. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

25. *The byzantine generals problem.* **Lamport, Leslie, Shostak, Robert and Pease, Marshall.** 3, 1982, ACM trans. Program. Lang Syst, Vol. 4, pp. 382-401.

26. *Performance Modeling of PBFT Consensus Process forPermissioned Blockchain Network (Hyperledger Fabric).* **Sukhwani, Harish, et al.** [ed.] IBM Corporation. Hong Kong : s.n., September 26, 2017, IEEE 36th Symposium on Reliable Distributed Systems.

27. **Salimitari, Mehrdad and Chatterjee, Mainak.** *A Survey on Consensus Protocols in Blockchain forIoT Networks.* Department of Computer Science, University of Central Florida. Orlando : s.n., 2019. p. 6.

28. **Cointelegraph.** Cointelegraph.com. [Online] 2018. https://cointelegraph.com/bitcoin-cash-for-beginners/what-is-hard-fork.

29. **Evans, Dave.** *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.* Cisco Internet Business Solutions Group (IBSG). 2011.

30. *Preserving Data Integrity in IoT Networks Under Opportunistic Data Manipulation.* **Bhattacharjee, Shameek, et al.** Orlando : IEEE, 2017. 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and

Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress. pp. 336-453.

31. *Fog Computing and Its Role in the Internet of Things.* **Bonomi, Flavio, et al.** [ed.] Cisco. Helsinki : s.n., August 17, 2012, Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing.

32. *A Cloud-based Architecture for the Internet of Things targeting Industrial Devices Remote Monitoring and Control.* **Silva, Ademir, et al.** s.l. : IBM Research, 2016. IFAC Conference Paper Archive. pp. 108-113.

33. *Fog computing for the internet of things: Security and privacy issues.* **Alrawais, Arwa, et al.** 2, IEEE Internet Computing, Vol. 21, pp. 34-42.

34. *Edge Computing: Vision and Challenges.* **Shi, Weisong, et al.** 5, s.l. : IEEE, October 2016, IEEE Internet of Things Journal, Vol. 3.

35. **Linthicum, David.** Edge computing vs. fog computing: Definitions and enterprise uses. [Online] Cisco. https://www.cisco.com/c/en/us/solutions/enterprise-networks/edge-computing.html.

36. *Design aspects for a reference M2M communication platform for Smart Cities.* **Elmangoush, Asma, et al.** [ed.] IEEE. Abu Dhabi : s.n., 2013. 2013 9th International Conference on Innovations in Information Technology (IIT).

37. *On the Convergence of Blockchain and Internet of Things (IoT) Technologies.* **Maroufi, Mohammad, Abdolee, Reza and Tazekand, Behzad Mozaffari.** March 11, 2019, ArXiv preprint .

38. *Constraints in the iot: the world in 2020 and beyond.* **Haroon, Asma, et al.** 11, 2016, International Journal of Advanced Computer Science and Applications, Vol. 7, pp. 252-271.

39. *Blockchain-Powered Internet of Things, E-Governance and E-Democracy.* **Qi, Renming, et al.** Singapore : Springer Nature, 2017, E-Democracy for Smart Cities, pp. 509-520.

40. **Patel, Keyur and Patel, Sunil.** Internet ofThings-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Enineering Science and Computing.* May 2016, Vol. 6, 5.

41. **Grand View Research.** *Industrial Internet of Things (IIoT) Market Size, Share & Trends Analysis Report By Component, By End Use (Manufacturing, Energy & Power, Oil & Gas, Healthcare, Logistics & Transport, Agriculture), And Segment Forecasts, 2019 - 2025.* 2019.

42. **International Data Corporation.** *Worldwide Semiannual Internet of Things Spending Guide .* Framingham Massachussetts : s.n., 2018.

43. **IoT Analytics.** State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. [Online] Market Insights For the Internet of Things, August 8, 2018. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

44. *Leading the iot, gartner insights on how to lead in a connected world.* **Hung, Mark.** 2017, Gatner Research, pp. 1-29.

45. **IoT Analytics.** *IoT platforms The central backbone for the Internet of Things.* s.l. : IoT Analytics GmbH, 2015.

46. **DBS Group Research. Equity.** *Regional Industry Focus Internet of Things.* 2018.

47. **Rogers, Everett Mitchell.** *Diffusion of innovations.* s.l. : Simon and Schuster, 2010.

48. *Architecture for the Internet of Things (IoT): API and interconnect.* **Grønbæk, Inge.** [ed.] IEEE. 2008. Second International Conference on Sensor Technologies and Applications. pp. 802-807.

49. *Internet of Things: Principles and paradigms.* **Rajkumar, Buyya and Vahid Dastjerdi, Amir.** s.l. : Elsevier, 2016.

50. *NanoPeer Networks and P2P Worlds.* **Triantafillou, Peter, et al.** Linkoping : IEEE, September 15, 2003, Peer-to-Peer Computing, International Conference on, p. 40_46.

51. **Microsoft Threat Intelligence Center (MSTIC).** blog.microsoft.com. [Online] August 5, 2019. https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/.

52. **Doffman, Zak.** Forbes. *Microsoft Warns Russian Hackers Can Breach Secure Networks Through Simple IoT Devices.* [Online] August 5, 2019. https://www.forbes.com/sites/zakdoffman/2019/08/05/microsoft-warns-russian-hackers-can-breach-companies-through-millions-of-simple-iot-devices/#20e1d2b3617f.

53. **Cimpanu, Catalin.** New Silex malware is bricking IoT devices, has scary plans. *ZDNet.* June 25, 2019.

54. **Climpanu, Catalin.** BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices. *Bleeping Computer.* [Online] December 11, 2017. https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/.

55. **Whittaker, Zack.** Homeland Security warns of 'BrickerBot' malware that destroys unsecured internet-connected devices. *ZDNet.* [Online] April 19, 2017. https://www.zdnet.com/article/homeland-security-warns-of-brickerbot-malware-that-destroys-unsecured-internet-connected-devices/.

56. **Bloomberg.** The Possible Vendetta Behind the East Coast Web Slowdown. [Online] October 21, 2016. https://www.bloomberg.com/news/articles/2016-10-21/internet-service-disrupted-in-large-parts-of-eastern-u-s.

57. **4New York.** 3rd Cyberattack 'Has Been Resolved' After Hours of Major Outages. 2016.

58. **Perlroth, Nicole.** Hackers Used New Weapons to Disrupt Major Websites Across U.S. *The New York Times.* October 21, 2016.

59. **BBC.** Cyber-attack: Europol says it was unprecedented in scale. *BBC News.* [Online] May 13, 2017. https://www.bbc.com/news/world-europe-39907965.

60. **Field, Matthew.** WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled. *The Daily Telegraph.* October 11, 2017.

61. **Smart, William.** *Lessons learned review of the WannaCry Ransomware Cyber Attack.* London : NHS Department of Healt & Social Care, 2018.

62. **NG, Alfred.** Cnet. *Justice Department charges North Korean over WannaCry.* [Online] September 6, 2018. https://www.cnet.com/g00/news/justice-department-charges-north-korean-hacker-linked-to-wannacry-2014-sony-hack/?i10c.ua=1&i10c.encReferrer=&i10c.dv=1.

63. **Proofpoint.** Proofpoint Uncovers Internet of Things (IoT) Cyberattack. [Online] January 16, 2014. https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack.

64. **IBM.** *Watson IoT and Blockchain:Disruptor and game changer.* IBM Watson IoT. 2017.

65. **Volkswagen.** From mine to factory: Volkswagen makes supply chain transparent with blockchain. [Online] April 23, 2019. https://www.volkswagen-newsroom.com/en/press-releases/from-mine-to-factory-volkswagen-makes-supply-chain-transparent-with-blockchain-4883.

66. —. Volkswagen Over The Air Update PoC With IOTA At Cebit 2018. [Online] August 23, 2019. https://iota-news.com/volkswagen-over-the-air-update-with-iota-at-cebit-2018/.

67. **Porsche Newsroom.** Blockchain: the key technology of tomorrow. [Online] January 11, 2019. https://newsroom.porsche.com/en/company/porsche-blockchain-technology-opportunities-digitization-16800.html.

68. **HYPR.** Blockchain meet biometrics.. HYPR and BITGO team up. [Online] March 03, 2016. https://www.hypr.com/blockchain-meet-biometrics-hypr-and-bitgo-team-up/.

69. **Chester, Jonathan.** How Blockchain Startups Will Solve The Identity Crisis For The Internet Of Things. *Forbes.* [Online] April 28, 2017. https://www.forbes.com/sites/jonathanchester/2017/04/28/how-blockchain-startups-will-solve-the-identity-crisis-for-the-internet-of-things/#545aa33d5c63.

70. **Digiconomist.** Bitcoin Energy Consumption Index. [Online] 2019. https://digiconomist.net/bitcoin-energy-consumption.

71. *Hybrid-IoT: Hybrid blockchain architecture for the Internet of Things - PoW Sub-blockchains.* **Sağırlar, Gökhan, et al.** [ed.] IEEE. Halifax, Canada : s.n., 2018. 2018 IEEE

Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing,. pp. 1-11.

72. **Allison, Ian.** Accenture Tech Now Connects Corda, Fabric, DA and Quorum Blockchains. [Online] October 22, 2018. https://www.coindesk.com/accenture-launch-interoperability-node-connects-corda-fabric-da-and-quorum-blockchains.

73. **Voshmgir, Shermin.** Blockchainhub. [Online] July 2019. https://blockchainhub.net/blockchain-oracles/.

74. **Coinbase.** Around the Block #3: analysis on the bZx attack, DeFi vulnerabilities, the state of debit cards in crypto, and other crypto news. *Coinbase blog.* [Online] March 13, 2020. https://blog.coinbase.com/around-the-block-analysis-on-the-bzx-attack-defi-vulnerabilities-the-state-of-debit-cards-in-1289f7f77137.

75. **Zainuddin, Aziz.** masthercrypto.com. [Online] 2019. https://masterthecrypto.com/blockchain-scalability-solutions-crypto-scaling-solutions/.

76. **Skidanov, Alexander.** Medium. [Online] December 12, 2018. https://medium.com/nearprotocol/unsolved-problems-in-blockchain-sharding-2327d6517f43.

77. **Glintborg, Mathias.** Medium. [Online] May 11, 2019. https://medium.com/ontologynetwork/ontologys-chain-network-for-businesses-scalability-and-performance-2fa971dff3dd.

78. **Debus, Julian.** *Consensus methods in blockchain systems.* Blockchain Center, Frankfurt School of Finance & Management. 2017.

79. **Fahad, Saleh.** *Blockchain without waste: Proof-of-stake.* Desautels Faculty of Management, McGill University. 2019.

80. *Proof of authentication: IoT-friendly blockchains.* **Puthal, Deepak and Mohanty, Saraju .** December 28, 2018, IEEE potentials.

81. **The European Union Blockchain.** *Scalability Interoperability and sustainability of blockchains.* ConsenSys AG. s.l. : EUBlockchain, 2019. pp. 1-29.

82. *A Multiple Blockchains Architecture On Inter-Blockchain Communication.* **Luo, Kan, et al.** Lisbon : IEEE, 2018. 2018 IEEE International Conference on Software Quality, Reliability and Security Companion.

83. **Clearmatics.** *Ion Stage 2: Toward a General Interoperability Protocol .* [Online] August 30, 2018. https://medium.com/clearmatics/ion-stage-2-toward-a-general-interoperability-protocol-part-1-d12b9d7316d3.

84. **ICON Foundation.** Blockchain Interoperability Alliance: ICON x Aion x Wanchain. [Online] December 5, 2017. https://medium.com/helloiconworld/blockchain-interoperability-alliance-icon-x-aion-x-wanchain-8aeaafb3ebdd.

85. **Higgins, Stan.** New Alliance Sets Out to Boost Blockchain Interoperability. *Coindesk.* November 28, 2017.

86. **The Ontology Team.** Ontology and NEO Come Together to Build an Open Cross-Chain Platform for Next-Gen Internet. [Online] July 18, 2019. https://medium.com/ontologynetwork/ontology-and-neo-come-together-to-build-an-open-cross-chain-platform-for-next-gen-internet-bd8e530bed8a.

87. **Schnorr , Clauss Peter.** Efficient signature generation by smart cards. *Journal of cryptology.* April 3, 1991, pp. 161-174.

88. **PR Newswire.** PR Newswire. [Online] June 23, 2020. https://www.prnewswire.com/news-releases/bsn-integrates-chainlink-oracles-bringing-real-world-data-into-its-irita-powered-network-301081572.html.

89. **Day, Allen.** Building hybrid blockchain/cloud applications with Ethereum and Google Cloud. [Online] June 13, 2019. https://cloud.google.com/blog/products/data-analytics/building-hybrid-blockchain-cloud-applications-with-ethereum-and-google-cloud.

90. **SWIFT Banking System.** *Bridging DLT and Smart Contracts with the SWIFT Network and Existing Bakn Systems.* Sibos. 2017.

91. **Gartner Research.** Cool Vendors in Blockchain Applications, 2017. [Online] May 04, 2017. https://www.gartner.com/en/documents/3698947.

92. **Forbes.** *Cornell's Town Crier Acquired By Chainlink To Expand Decentralized Oracle Network.* [ed.] Darryn Pollock. November 1, 2018.

93. **IOTA Foundation.** The Coordicide. [Online] May 2019. https://files.iota.org/papers/Coordicide_WP.pdf.

94. —. IOTA blog. [Online] August 19, 2020. https://blog.iota.org/chrysalis-iota-1-5-phase-1-now-live-on-mainnet-958ec4a4a415.

95. **IOTA archive.** List of industrial and institutional interest in IOTA. *The IOTA ecosystem tracker.* [Online] 2019. http://iotaarchive.com/listing.html#/.