Available online at http://www.ijims.com
ISSN - (Print): 2519 – 7908 ; ISSN - (Electronic): 2348 – 0343
IF:4.335; Index Copernicus (IC) Value: 60.59; Peer-reviewed Journal

Blockchain to succeed IoT in Smart City – State of the art

* Zakariae Dlimi
LAVETE Laboratory
FST/Univ Hassan I
Settat Morocco

Abdellah Ezzati
LAVETE Laboratory
FST/Univ Hassan 1
Settat Morocco

Saïd BEN ALLA
LAVETE Laboratory
FST/Univ Hassan 1
Settat Morocco

*Corresponding Author: Zakariae Dlimi

Abstract

Internet of things (IoT) refers to the concept of all digital technologies being able to connect and interoperate with each other, in order to solve several problems that currently exist in the physical, economic and social fields of our daily lives. These problems may be the need for automation to provide efficiency and high levels of accuracy, the need to provide several services or for visibility that will allow manufactures to acquire feedback from their customers, wich will hence lead to tailoring of products to the specific needs of customers. IoT aims at providing a framework to integrate all objects, smart devices, machines, patients, consumers and several services into one interconnected network. In order to achieve these goals IoT will require to employ a vast array of technologies that will be able to sustain its high data traffic and processing power as seen by the number of devices connected estimated to be 50 billion by 2020. The modular approach to IoT will require that each of these devices to be integrated with sensors such as GPS, RFID or scanner and connect them through the Internet using specific protocols for communication and data transfer. Blockchain (BC) technology refers to a distributed public ledger system that keeps records as a chain of interconnected blocks that start from a genesis block - first block to be added in the chain. BC technology aims at creating a decentralized trustless environment where transactions and data are not in the control of any third party.

Keywords IoT; Smart city; Blockchain

1 Introduction

The concept of IoT Smart City is a comprehensive framework that addresses the requirements for multiple Smart City projects that enable these cities to use urban networking in order to increase its economic strengths, improve on technology and to provide more efficient solutions to counter many of these city's challenges. These challenges may be the need to improve living standards, optimizing consumption of available resources, reducing risks or improving governance. A smart city refers to a city that connects all physical infrastructure, communication and information technology infrastructures, social infrastructure and business infrastructure to increase the collective intelligence of the city. IoT in more technical sense can be defined as Objects with virtual identities and personalities in intelligent spaces, and using intelligent interfaces to connect and communicate with social, medical, environmental and user contexts. IoT aims at leveraging the power of embedded sensors and actuators in different objects and machines to gather data, which is then analyzed in order to improve on services and products, or to automate systems. IoT is expected to grow in coming years, which will provide a new dimension in the quality of services, better consumer conditions and increased productivity of enterprises. Consumers of products and services are said to benefit in that IoT will provide solutions that will improve energy efficiency, health, education and security, just to mention a few of the areas expected to scale up with the incorporation of IoT.

Mobile networks account for the connectivity of a large range of devices which goes beyond the tablets, phones and laptops, to connected buildings, cars; game consoles and TVs; traffic controls and smart meters and still provide a huge untapped potential to connect almost everything and anyone. The number of those connected device is estimed to be 50 billion by 2020 [1]. The potential of this connection is evident as seen in the development of new innovative services and applications in every sector of human life. The evolution of IoT depends majorly on the coordination of multiple vendors devices, machines and appliances that are then all connected together to the internet using different networking technologies and optimizing strategies.

Although the expected impact of IoT is revolutionary, much effort still needs to be put so that to move from this early stage in order to unlock the full potential of IoT. Efforts are being made around interoperability, standardization, Big Data management, network management, artificial intelligence-assisted management, etc. The Blockchain technology, which fits into the technical as well as the business axis, brings several gains to the IoT and Smart City platform, namely security, decentralization, trust layer, orchestration, interoperability and new business models that allow stakeholders to think of new use cases that before were difficult to implement.

The preceding chapters will be organized as 2. State of the art IoT and smart city, 3. State of the art Blockchain, 4. Integration of Blockchain and IoT in Smart city, 5. Conclusion and 6. Future work.

2 State of the art of IoT and smart city

Smart cities are cyber-physical ecosystems that are being developed by deploying novel services and advance communication infrastructure over city wide scenarios. Smart city domains major on optimizing the sustainability of the physical city infrastructures such as power grids, road networks and improving the living standards of its citizens. Smart cities offer diverse applications such as smart homes and environmental monitoring.

In smart homes or buildings sensors and actuators are installed to monitor resource consumption and optimizing performance of the controlled resources according to user needs. An example can be switching on/off of lighting and heating tasks. These applications offer advantages in reducing resource consumption within the building such as electricity and water and also reduce the carbon emission associated with buildings, reducing global greenhouse gas emission.

In environmental monitoring, natural phenomena and processes such as temperature, wind, rainfall and water levels in rivers and lakes are monitored using applications that have the ability to sense these environmental factors. These applications have the ability to handle and process large amount of heterogeneous data collected from sensors in real time, and thus provide a rapid response reducing the damage that would otherwise be caused to buildings, nature or people. Examples of these applications include fire detection and natural disaster detection e.g. tsunamis, tornados and earthquakes.

In smart cities, IoT solutions help improve infrastructure, create more efficient citizen services, reduce traffic congestion, and improve people’s security. To unlock the full potential of IoT, smart cities stakeholders recognize that this cities should not offer a separate smart solutions, but delivers a whole scalable and secure IoT framework solution that includes useful IoT systems.

A smart city solution must provide the possibility to manage all the components namely the millions of connected people and devices, and systems. The solution must also enable to integrate the technological requirements of today's IoT[2]. More precisely, an IoT Platform should be able to connect different heterogeneous systems of the city, reduce the time to set up IoT services, create value from data around connected devices, deliver a scalable and secure access service and open the possibility to the new opportunities of the city

The deployment of IoT smart cities needs different architectures, interaction protocols, technologies and communication standards that work perfectly among the different objects. Several global organizations are involved which include: IEEE, ITU, IETF, GS1, OASIS, and many others.

2.1 Architecture of IoT

IoT architectures present a structure and standard concepts that are able to actualize the essential building blocks for IoT basic architectures, and that facilitate the interoperability between heterogeneous systems. IoT will have to incorporate several technologies due to vast array of objects connected such as near field communication (NFC), radio frequency identification (RFID) and wireless sensor and actuators networks (WSANs). Moreover, IoT involves the use of different protocols, data formats and communication standards making the IoT environment decentralized, complex and heterogeneous. This brings up the need to define the architectures and standards at different levels of abstraction in the IoT environment. IoT architectures introduce an abstract framework that lists a minimum set of unifying concepts, relationships and axioms that gives a better understanding of the relationship between the entities of the IoT environment. Due to the heterogeneous nature of IoT, one architecture cannot be used but instead several IoT architectures coexist for the diverse need of IoT implementation.

Due to the ongoing development and evolution of protocols, standards and application contexts, several types of IoT architecture are proposed. RFC 7452 describes four communication models for IoT.

2.1.1 Device to Device from different providers on the same network (figure 1)

In general, the devices are manufactured by different manufacturers. These devices require interoperability to communicate directly with each other. This forces manufacturers to agree on the same protocols, data model, encoding, IP configuration and security.

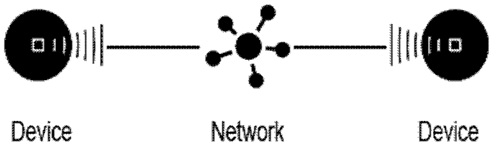

Figure 1: Device to device in the same network

2.1.2 Device to Cloud (figure 2)

In this model, the devices and the cloud service can come from the same provider. Devices send data to a single application, where data is collected and analyzed for centralized monitoring and control. Devices can benefit from TCP / IP, http, UDP.

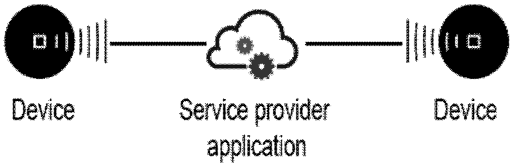

Figure 2: Device to Cloud

2.1.3 - Device to the gateway of the Application Layer (figure 3)

This model allows you to direct your use to the "Device to Cloud" model by connecting non-IP devices to the cloud service, via the gateway that provides interoperability. The communication between the gateway and the Cloud service goes through IP4 / IP6.

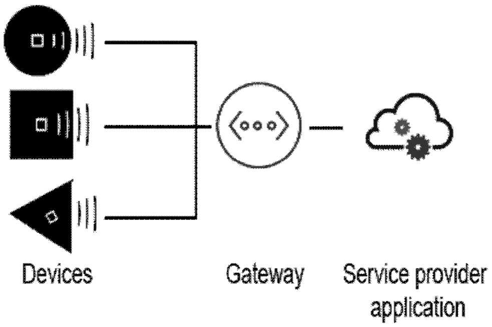

Figure 3: Device to Gateway

2.1.4 - Back-end for data management

The principle is to allow devices to upload their data to third-party applications in order to aggregate them with other sources and analyze them for specific user needs. The basic architecture is organized in 3 layers *(figure 4)*: Perception layer: for understanding data collected through physical objects, Network Layer: For data collection of devices and their transmission to the Application layer, e.g. via 3G, Wi-Fi, ZigBee, NFC, etc. and Application Layer: For processing and decision services.

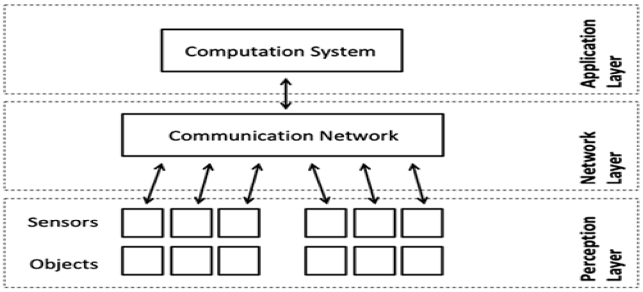

Figure 4: Basic architecture in 3 layers

This architecture has been further developed by adding a fourth service layer where actions are taken and also another architecture which introduces a sixth mac layer for energy management and devices supervision.

2.2 Challenges and constraints to succeed the IoT smart city

Internet of Things promises the interconnection of a myriad of smart things that will be deployed worldwide to provide services to people and things. However, the traditional Internet architecture based on sharing resources design is not appropriate for Internet of things based on sharing data. Some open challenges are listed below:

a. *Security*: One of the most important challenges is security which concerns privacy, integrity, availability and encryption. Objects are deployed in large scale in IoT environments and given the existing security architecture is designed from the perspective of people communication, it does not suitably cater for IoT systems. Data integrity, privacy, data ownership, energy-efficient cryptography algorithms, legal and liability issues have to be addressed accordingly.

b. *Orchestration*: The development and deployment of self-aware systems, autonomic systems with self-properties enabled, is a challenge due to the specific characteristics of IoT environments. IoT environments presents a pool of heterogeneous objects using different technologies and data formats from their manufactures and thus autonomous systems have to interoperate with these technologies which present a challenge given the number of devices.

c. *Interoperability*: Technological and semantic interoperability is significantly more complex for IoT environments than for the traditional Internet environment due to their different technological specifics, and their ability to relate people to objects and objects with objects This seamless interaction between people with heterogeneous devices generates a large amount of shared heterogeneous information. Thus, improvements have to be made regarding the information model to the devices, interpret the shared information correctly and act accordingly. Moreover, for full interoperability, standards for IoT must be created and broadly used. IoT reference architectures should be defined then, IoT concrete architectures must be specified based on such IoT reference architectures. This standardization can facilitate the interoperability between heterogeneous IoT systems.

d. *QoS*: By default, IoT is multi-service, providing different applications or services. Thus, multiple traffic types (e.g., throughput and delay tolerant elastic traffic classes) will be transmitted within the network, and many applications/services will need quality of service (QoS) compromise. Moreover, IoT involves shared wireless media, data, and tools available on clouds, which is already an environment needs QoS requirements. Therefore, providing quality of service in IoT environments can be a hard challenge.

e. *Big data:* A large amount of data will be transmitted from (billion or trillion) heterogeneous things to the IoT. Exploring the large volumes of data and extracting useful information from a complex sensing environment at different spatial and temporal resolutions in a fast and effective way is a challenging research problem. The key characteristics of resource constraints in sensor networks (and RFID systems) and high capacity for applications in cloud computing create novel challenges for proposals of adaptive and distributed solutions.

f. *Constrained capacity:* In general, heterogeneous sensing devices taking part in the IoT demands the use of multiple sensing modalities and are not connected to an unlimited power supply. Therefore, efficient energy sensing is a conditioning factor in the design and operation of IoT environments. Therefore, many IoT solutions based on WSN or RFID have to be oriented to low-energy consumption. While such technologies do not still provide enough resources, this is a broad research challenge. Approaches proposed for WSNs and other low-power technologies can be adapted to deal with the requirements of the IoT.

2.3 Interaction protocols to connect things

Several protocols have been researched on and proposed by different organizations and stakeholders to interconnect objects and end user applications to the Internet of things. These protocols include MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol) and WAMP (Web Application Messaging Protocol).

2.3.1 Messaging queuing Telemetry Transport (MQTT) is an open messaging protocol created for machine-to-machine (M2M) communication, to address issues related to high latency, unstable communication, and low bandwidth. MQTT employs TCP as its communication protocol, and the publisher/subscriber paradigm as it messaging pattern [3][4].
2.3.2 MQTT-SN is an extension of the MQTT protocol used on embedded devices that communicate on non-TCP networks and instead uses the UDP protocol [3][4].
2.3.3 Constrained application protocol (CoAP) was created based on the HTTP RESTful architecture to allow highly constrained devices to be accessible through URLs and allow clients to use methods like GET, PUT, POST, and DELETE. Standardization of CoAP was done in 2014 by IETF as RFC 7252, and it was
designed to be extensible, with some other RFCs implementing additional functionalities
2.3.4 Extensible Messaging and Presence Protocol (XMPP) was created in 1998 aimed to be an open technology for instant messaging services, using XML streaming at its core.
2.3.5 Web Application Messaging Protocol (WAMP) goal is to be a "Unified Application Routing", uniting the publisher/subscriber (Pub Sub) model with remote procedure calls (RPC), over the
WebSocket protocol [5].

2.4 Cloud layer to manage the whole data

Cloud Computing is a concept in which companies and individuals are able to rent processing and storage capacity, instead of making big investments to construct and provision a large-scale computing platform [6]. These services are typically hosted in data centers, using shared hardware for processing and storage. Elasticity, scalability, economies of scale and pay-per-use pricing are the major reasons for the successful and widespread adoption of cloud infrastructures. One major benefit claimed for cloud computing is elasticity, that adjusts the system's capacity at runtime by adding and removing resources without service interruption in order to handle the workload variation [7]. On the other hand, the Internet of Things (IoT) represents a worldwide network of heterogeneous cyber-physical objects such as sensors, actuators, smart devices, smart objects, RFID, embedded computers. In general, the devices on the IoT have resource constraints and, therefore, are traditionally designed to support specific applications. The strong coupling between the network and the application limits the use of resources and data collected by the devices. IoT is made up of numerous heterogeneous devices, technologies, and protocols. Therefore, scalability, reliability, interoperability, security, efficiency and availability can be very difficult to acquire. The integration with the Cloud solves most of these problems [8], also providing additional features such as ease-of-access, ease-of-use, and reduced deployment costs. cloud computing can be customized to support a distributed real-time system for the management and analysis of IoT things and data streams generated by IoT things. Cloud computing also presents a solution to IoT big data challenge characterizing the IoT environment due to the large number of devices connected. These data can be efficiently and optimally processed by the infrastructure provided by the cloud.

2.5 Fog & Edge computing to improving Cloud layer

Fog Computing is a concept that extends Cloud computing and services to the network edge. Fog can be differentiated from Cloud by its proximity to end-users. According to the authors [9], fog computing is:
« Fog computing is a scenario where a huge number of het- erogeneous (wireless and sometimes autonomous) ubiquitous and decentralised devices communicate and potentially cooperate among them and with the network to perform storage and processing tasks without the intervention of third parties. These tasks can be for supporting basic network functions or new services and applications that run in a sandboxed environment. Users leasing part of their devices to host these services get incentives for doing so. »
The emerging trends in networking such as large distributed Internet connected sensor networks (IoT), mobile data networks, and also real-time streaming applications have specific requirements that cannot be satisfied by cloud computing. Fog provides compute, storage and network similar to Cloud. In contrast to the cloud, Fog presents specific characteristics: edge location and location awareness implying low latency; geographical distribution and a vast number of nodes in contrast to centralized Cloud; support for mobility through wireless access and improves the quality of service (QoS) and real-time applications. Thus, fog computing is the most suitable communication model compared to cloud computing where information processing takes place within the internet and provides faster transfer of data [10]. These improvement in characteristic has inspired the development of many scenarios, such as smart grid, vehicular networks, wireless sensor networks, IoT, and software-defined networks (SDNs) that require faster processing with less delay and real-time interactions.
For situations requiring high predictability latency and reliability, the goal should be to locate the intelligence where it is needed in the network, or even be embedded on them, thereby enabling higher reliability and localized closed loop control. It improves the processing and storage of data for analysis
and making real-time decisions essential for many applications. To increase the use of Fog computing, it is necessary to address some challenges, such as programmability, accountability, standardization, management, discovery/sync, compute/storage limit and security.
Edge computing refers to the use of edge node resources such as CPU, memory and storage to process several network functions that would otherwise be performed centrally by the cloud infrastructure. This has the effect of reduced communication latencies and traffic to

the cloud. However, the edge has limited resources and thus presents the need for several optimization strategies to maximize on these resources in order to optimize network performance [11].

While solutions exist, the multiplicity of actors also imposes constraints to agree on standards of communication protocol, technological base, and deployment. A platform that will bring several solutions at once, will reduce these constraints cited that Smart City meets, hence the idea of using the Blockchain, a technology that can bring autonomy and intelligence through the use of smart contracts, disintermediation by non-need for trusted third parties, security through its algorithms, and the distribution and decentralization of the system.

In this next chapter, we will present a view of Blockchain technology, its relationship with IoT in the Smart City, and current considerations for its integration.

3 State of the art of Blockchain

Blockchain technology is an irreversible, encrypted, decentralized ledger that has the potential to make all centralized activities, processes, and organizations entirely autonomous [12]. Its most famous application is Bitcoin, a cryptocurrency with a capital market that reached 320 billion in 2017 [13]. The Blockchain technology was proposed in 2008 to address the problem of double spending of digital currencies and was first implemented in 2009 for Bitcoin [14]. Since then the technology has seen much interest and is constantly evolving for economic and technology interest. The Blockchain can be viewed as a public ledger where all transactions are stored as a series of blocks, protected by asymmetric encryption and distributed consensus algorithms. The Blockchain can be applied in different areas, such as payment, utilities, the Internet of Things, and security services.

Recently, the Internet of Things has brought up the need for advanced automation, where the network nodes which include devices and sensors are all interconnected. The majority of these devices are limited in terms of resources, which makes it difficult to implement heavy cryptographic approaches. Recent research has shown that the use of the Blockchain in the field of IoT provides a real security solution. The IoT ecosystem follows a centralized system architecture for device management, identification and authentication, which presents a problem of scalability. As a result, the Blockchain can serve as a solution to this scalability problem by bringing privacy and management gains through its distributed authentication and management system which characterizes a distributed and decentralized IoT ecosystem.

3.1 Features of the Blockchain

Blockchain is a distributed database system that is based on consensus algorithms which allows the transfer of value between entities. There exist several distributed databases based on consensus algorithms, however, Blockchain has three distinctive features [15][16]:

g. Permission less: On the Blockchain network, there is no central governing body that decides who can operate on the network and who cannot. Anyone can operate in the network.
h. Trust less: No one on the Blockchain network has to own a certified digital identity. The involved entities do not know each other nevertheless they can exchange data with each other.
i. Censorship resistant: Blockchain is a network without controllers where participating entities only trust on cryptographic algorithms that govern the operation of the network. An operation once completed and accepted cannot be reversed.

Blockchain can also be categorized as permissioned and permission less depending on functionality [15]:

j. Permissioned: permissioned Blockchains limits users who can participate on consensus of the system state. Only allowed users can participate in achieving consensus of the system state. It may also limit users who can initiate smart contracts.
k. Permission less: permission less Blockchains allows anyone to join the network, participate in the process of block verification to reach a system consensus and also create smart contracts.

3.2 The structure of the Blockchain

Blockchain structure is based on four concepts:

l. Peer to peer network: Nodes participating in a Blockchain network communicate directly to each other without the need of a trusted third party. Each node in the network has the same privileges and interacts with the others by using a pair of public and private keys. The public key act as an address to be reachable on the network while the private key is used to sign transactions.
m. Open and distributed ledger: The ledger is a record of all transactions in the network. The ledger is not stored at a centralized location but each node has a copy of the ledger. The ledger can be accessed and read by each node in the network and nodes can determine whether transactions are valid or not.

n. Ledger copies synchronisation: since every node has its own copy of the ledger, this brings an issue of how the chain should be updated on all the nodes without loosing its structure and integrity. This is achieved through three steps: new transactions are broadcast to the entire network, validation of the new transaction and finally adding the block into the chain.

o. Mining: due to resource bottlenecks, which cause network delays, not all nodes receive transactions at the same time. Blockchains must have a valid and ordered branch and because of this each node in the network cannot be allowed to add blocks to the chain. Miners are special nodes that are tasked with adding blocks to the chain. Miners compete with each other to acquire transactions, validate them and add them to the Blockchain. The first to add a block and is validated is rewarded with a token.

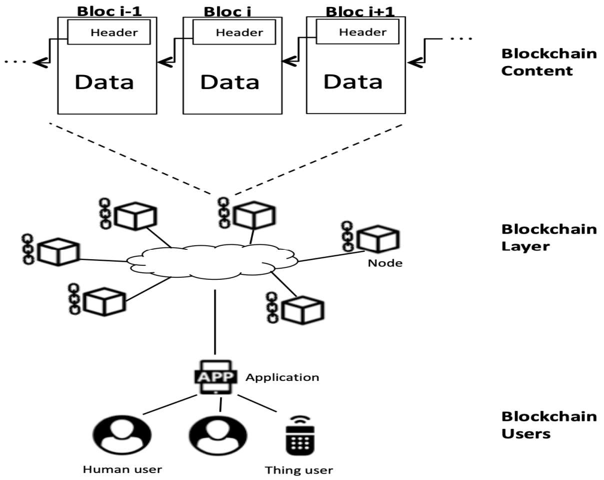

Figure 5: Overview on the Blockchain system

Blockchains are made of a connected chain of blocks of transactions performed in the network. The blocks contain the following information:

p. Header: It consists of a timestamp, target of the consensus algorithm e.g. PoW, the hash value of the previous block HEADER, which acts as a cryptographic link linking the chain in order to make it tamper-proof, Merkle tree root, which encodes the transactions in the block in a single hash code with leaves representing data blocks accumulating since the Blockchain was created from the genesis block and nonce, which is required for solving the PoW, which also serves to prevent a replay attack.

q. Block Content: It consists of all the inputs and outputs of each transaction. The input data contains the output of the previous transactions and an address containing the signature with the private key of the owner which acts as ownership proof of such an asset. There are two concepts for managing the assets of an address: The unspent transaction output model (UTXO), and the Account balance model. The output data contains the tokens to be sent and the address of the recipient (the recipient's public key). The recipient will be the sole user, able to spend that asset because only his private key can prove the asset ownership. The content of the block, not only refer to financial transactions, the main reason for the creation of Bitcoin, but also can refer to other type of non-financial applications projecting to the use cases of the IoT environment. (information and data related to IoT devices, users of IoT services, etc.)

Each block that is approved is connected to the previous block (*figure 5*) using a cryptographic hash, which act as a unique and an immutable stamp, which guarantees that no one can tamper with the record.

3.3 Dynamics of the Blockchain

The operation of Blockchain differs from one type to another, according to different criteria, and precisely the mode of consensus. The dynamics of the Bitcoin Blockchain are presented below from a generic point of view:

a. A user proceeds to the creation of transfer transactions (address input to address output) and adds his signature

b. The user broadcasts the transaction request to the nodes of the network

c. Each node receives the transaction requests, checks them and processes up to the size limit, then creates a new block

d. Nodes are trying to solve the riddle of proof of work

e. After resolution, the node broadcasts the block in the network

f. Each node that received a block, checks it and adds it to its local Blockchain

g. As time goes by, a node readjusts its local Blockchain by the longest existing Blockchain that has been communicated to it.
h. A transaction is considered reliable when it is validated by at least 2 nodes. The degree of reliability increases by the number of validations by the nodes.
Signature and verification are provided by the asymmetric encryption mechanism. Each user has a randomly generated private key that allows transactions to be signed. Its public key, which is calculated from the private key (ECDSA Algorithm [17] in the case of the Bitcoin Blockchain) allows the node to verify the authenticity of the transaction issuer.

3.4 Consensus algorithms

By its characteristic of autonomous networks of nodes, the Blockchain is confronted with the problem of Byzantine generals, to ensure its smooth operation despite the defect of one or more nodes [18][19].
Byzantine Fault Tolerance (BFT) refers to fault tolerance of a distributed computing system where its nodes may be faulty or malicious. PBFT is the implementation of the Byzantine fault tolerance algorithm. The algorithm makes it possible to keep the network running smoothly unless more than 1/3 of the nodes are corrupted. This approach requires that the identity of each member be known, hence a centralized entity that manages this data. The consensus is orchestrated by a node that acts as the main server and provides communication between nodes in 3 phases, pre-preparation, preparation and commit. Nodes can change primary server if it is missing.
The Bitcoin network uses the consensus Proof of Work. This type of consensus presents a revolutionary concept and is considered as the major lever for the development of the network of a public Blockchain [18].
To add a new Block to the chain, special nodes called miners, tries to solve a puzzle whose difficulty increases by increasing the number of nodes in the network. The puzzle is hard to solve but easy to verify. As soon as a node finds the solution, it adds it to the contents of the block, the Hash and broadcast it in the network. When a node receives a new block, it checks the proof of work and adds it to its local chain. This approach is very computation intensive, and it takes more than half the computing power of all network nodes to corrupt it. To increase the number of blocks in the Blockchain with a PoW type of consensus, the nodes are rewarded for their work by generating new coins.
Several consensus algorithms are used to run several Blockchains. Examples include proof of stake, proof of storage, Algorand, ledger consensus protocol, Steller consensus protocol etc.

3.5 Smart Contracts

Nick Szabo introduced this concept in 1994 and imagined it as contractual clauses in the computer code that is able to apply them automatically to minimize reliance on trusted intermediaries between stakeholders [20]. In the context of the Blockchain, smart contracts have been implemented in the Ethereum platform as an evolution of the Bitcoin Blockchain technology, with stored scripts capable of executing processes during transactions [21]. The smart contract is stored in an address in the Blockchain, and can be triggered by sending a transaction to that address. Then, the contract is automatically executed on all the nodes of the network. In this way, the Blockchain network behaves like a distributed virtual machine.
Smart contracts have the following properties:

r. Autonomy: Participating entities agree on the decisions and thus intermediary and bias related decisions are eliminated.
s. Trust: Essential files are present on a public ledger and thus cannot be destroyed or lost.
t. Backup: data is stored on multiple nodes participating in the network making the data safe.
u. Savings: Smart contracts eliminate the need for a Trusted Third Party and thus save money

3.6 Deployment considerations

Despite the listed benefits of integrating the Blockchain into the IoT Smart City ecosystem, there are some limitations to consider when deploying.

3.6.1 Cost of encryption and consensus

Blockchain models such as Bitcoin that works through a Proof of Work (PoW) consensus mechanism require significant computational power for solving the challenge enigma. The time of the resolution also increases due to the increase of the difficulty of the enigma. This is constraining when it comes to connected devices of limited resources.

3.6.2 Architecture and integration

The architecture models of IoT systems in the Smart City ecosystem differ from provider to provider, and from context to context. The Blockchain model should be adapted to fit well into this heterogeneous world, with minimal interfacing effort for existing systems or for new opportunities.

3.6.3 Lightweight Blockchain ledger

Also, the Blockchain registry distribution model on the network nodes is not practical in an IoT ecosystem whose devices have limited resources, and in a Smart City ecosystem with huge data and size.

4 Integration of Blockchain and IoT & smart city

It is estimated that major of newly created devices by 2020, will be IoT enabled, making IoT in a large extend, to be part of our life experience. Everyone will be interacting with networked objects and business will be digitally transformed. Even though IoT present a platform for the development of innovative end user applications, challenges as security, scalability, interoperability, and data management become a major concern and if not checked will lead to several critical issues..

Blockchain technology on the other hand provides the technology to solve security, scalability, and interoperability problems associated with IoT. The distributed trust less characteristic of Blockchain that ensures scalability, privacy and reliability forms the foundation for the development of such IoT environments.

IoT presents several issues that may lead to a security breach. The first challenge comes from the fact that IoT is a distributed network and any single node in the network can be a point of cyber-attacks to the network. The second challenge comes about data confidentiality and authentication. The third challenge comes from data integrity where data is fed on autonomous system to aid in uncontrolled decision making. The basic features of autonomous trust less and decentralized features of Blockchains make it applicable in several scenarios such as smart industries, smart homes, smart grid and smart cities. Blockchains through the use of smart contracts can be used to create autonomous functioning of systems, keep an immutable history of smart devices and create a secure way of smart devices to exchange messages.

Despite the positive gain that Blockchain technology brings to IoT, standard implementations are energy and computationally intensive, scalability-limited, and generate significant traffic and response time. the author [22] offers Lightweight Scalable Blockchain (LSB), which is optimized for IoT prerequisites. LSB provides decentralization through the implementation of a high-capacity device overlay network, which manages a public Blockchain to enforce security and privacy. Thus, the exchange between the IoT devices is decorrelated from the recording of transactions in the Blockchain. The authors provided optimizations to LSB at the algorithm level for a lightweight consensus. The overlay network nodes are clustered, and only cluster heads (CH) are responsible for managing the Blockchain to reduce the number of blocks created. The block validation consensus is based on a distributed trust algorithm, which assigns a trust score to the CHs in the community. Also, for flow management, the author proposes a balancing mechanism between the number of transactions to add to the Blockchain and network load capacity, called Distributed troughput Management (DTM).

IoT access management solutions are based on centralized models, with technical limitations such as resource bottlenecks, single point of attack vulnerability, and single point failure network. An example of Blockchain integration in IoT environments is proposed by [23] aims at providing architecture for scalable access management in IoT. This architecture describes a new decentralized access management system where access control data is stored and distributed using Blockchain technology. Each entity will be part of Blockchain technology except for IoT devices and management hub nodes. All nodes in the Blockchain network must include a copy of the Blockchain. The Blockchain keep increasing over time and can be considerably large in size. The majority of IoT devices due to their constrained nature will not be able to store Blockchain information. Consequently, the proposed architecture does not include IoT devices in the Blockchain but rather defines a new node called Hub Manager that requests access control information from the Blockchain on behalf of IoT devices. This Hub Manager make gateway between IoT and Blockchain by transforming message from CoAP to JSON-RPC. Moreover, the solution involves a single smart contract in the access control system, which defines all the operations allowed. That contract is unique and cannot be deleted from the system. Entities called managers interact with the smart contract in order to define the access control policy of the system.

Drones see a lot of applications in the IoT environment in sectors such as agriculture, military and delivery services. The use of drones in these areas present several challenges such as vulnerable wireless networks for control and data transmission, limited resource of drones, challenge of data integrity and resilience. The authors [24] propose a distributed architecture Blockchain based technology, for the arbitration of roles and permissions in the drone network in IoT environments. This architecture aims to provide: Lightweight, scalability, accessibility, transparency, concurrency and isolated governance. In this architecture the network is divided into five key components: Drone, control system, Blockchain network, cloud database and cloud server. A cluster of drones may be delegated a single role and communicate with the control system either directly or through an intermediary drone. The control system is responsible for receiving collected data and sending out commands. It also send datas and their hashe to the cloud and Blockchain network respectively. Blockchain network stores the hashed data entry for integrity protection. The cloud server validates records stored in the cloud database by requesting the Blockchain network for receipts for data integrity and also can perform analysis of data for automation of control of the drones.

Cloud solutions bring a significant gain in the design of applications and IoT platform, for storage and processing, given the large number of devices that emerge. However, users have no choice but to trust the providers of these applications and the cloud services with the promise of security and availability, and have no way to verify and manage these conditions themselves. author [25] proposes a Blockchain-based data access control management system to ensure efficient auditability, secure data sharing, distributed storage, and search in fragmented and compressed data. The solution presents a distributed storage system consisting of Blockchain, virtual-chain, routing and storage. Blockchain and virtual-chain together form the control plane while routing and storage form the data plane. The network consists of transactions of ownership of data streams and their corresponding access rights. The Blockchain is used to store the access rights of the data stream. Access rights are granted per data stream and the owner of the data stream can revoke access to that data. For any request to retrieve data, storage first checks the access rights from the Blockchain. The data plane is presented with the challenge of IoT data compatibility, where IoT data streams are generated continuously given the number of connected devices.

An architecture proposed by [26], introduces a framework for forensic analysis of traffic accidents. The utilization of vehicle-related data collected from several sensors fitted on the vehicles can be instrumental in post-accident scenarios in order to discover the faulty persons or parts related. The framework connects several participants including: vehicles, vehicles manufactures, maintenance service providers, law enforcement and insurance companies. The architecture involves a daemon process stationed within the on board unit (OBU) and constantly collects data from the BSMS, EDR and other fitted sensors. Event data recorder (EDR) records data related to crashes and accidents including airbag deployment and sudden speed changes above a threshold. Basic safety message (BSM) captures high-priority data about a vehicle including position, speed, brake status, size and ID of the vehicle, and also medium-priority information such as positional accuracy and steering wheel angle. The forensic daemon process periodically shares the EDR and BSM information with the insurance company through an encrypted channel. BSMs related information is shared only when an EDR triggering event occurs. Vehicle manufacturers collect regular car diagnostic reports. A cryptographic hash of these data is forwarded to the Blockchain to provide integrity of data and remove the single trusted third party issue. Insurance companies and manufacturers collect these data for performance analysis. Moreover, maintenance service providers keep maintenance records, and a hash of each record is also sent to Blockchain. The Blockchain data is stored in a distributed ledger fragmented, consisting of knowledge domain. Each stakeholder of the system records only the data that interests him. The authors proposes the VPKI scheme for privacy and membership management.

LoRaWAN is a competitive technology that meets the need for IoT in the Smart City. However, since it is operated by private companies and organizations, it represents a trust risk between client applications and network operators. The author [27], proposes a solution to build an open, decentralized, reliable and inviolable system for LoRaWAN, based on the Blockchain technology, to verify that the data of the transaction has existed in the network to a specific time. The solution works by building a Blockchain network from the Network Servers (NS), which manage all the functionality of the Blockchain, transaction, encryption, block validation and storage of the ledger. This choice is justified by the fact that only the network server is able to play this role among the components of the LoRaWAN network.

5 Conclusion

The IoT industry faces many challenges such as energy consumption, network reach and security. In the Smart City dimension, other challenges also appear such as scalability, interoperability, governance, data management, and the security of all participants. The Blockchain by its design goal, to create a secure, trusted, autonomous, decentralized, and intelligent system, would solve many of the challenges faced in the IoT and Smart City. However, to succeed in its integration, it is necessary to rethink the mode of operation of the Blockchain for a reasonable energy consummation in the consensus mechanism, for a lightweight ledger, and for adaptability in the ecosystem of the IoT in the Smart City.

6 Future work

The Blockchain is a technology model that opens several technical and business opportunities in the context of Smart City connected objects. However, it is a young field that requires research for improvement and adaptation. Following this general view, our future work will focus on the modeling of a new Blockchain Framework, integrated in a context of IoT Smart City, and which improves limits cited in this article. Subsequently, we need to apply this Framework in practical contexts such as Smart Homes or Smart Transportation.

REFERENCES

[1] Dave Evans, 2011, Cisco Internet Business Solutions Group, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[2] Kavitha.R, Sumathi.P, A SURVEY ON THE INTEGRATION OF CLOUD COMPUTING WITH INTERNET OF THINGS: RESEARCH ISSUES, CHALLENGES, PLATFORMS AND APPLICATIONS FOR SMART CITIES. International Journal of Computer Engineering and Applications, Volume XII, Issue VII, July 18, www.ijcea.com

[3] Ian Skerrett. Case Study MQTT: Why Open Source and Open Standards Drive Adoption, https://ianskerrett.wordpress.com/2015/03/04/case-study-mqtt-why-open-source-and-open-standards-drives-adoption

[4] MQTT Version 3.1.1 OASIS Standard, http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

[5] The Web Application Messaging Protocol, http://www.ietf.org/internet-drafts/draft-oberstet-hybi-tavendo-wamp-02.txt.

[6] Ribas, M., Furtado, C. G., de Souza, J. N., Barroso, G. C., Moura, A., Lima, A. S., & Sousa, F. R. C. (2015). A Petri net-based decision-making framework for assessing cloud services adoption: The use of spot instances for cost reduction. Journal of Network and Computer Applications, 57, 102–118.doi:10.1016/j.jnca.2015.07.002

[7] E. F. Coutinho, F. R. de Carvalho Sousa, P. A. L. Rego, D. G. Gomes, and J. N. de Souza. Elasticity in cloud computing: a survey. annals of telecommunications-annales des télécommunications, 70(7-8):289–309, 2015.

[8] Fortino, G., Guerrieri, A., Russo, W., & Savaglio, C. (2014). Integration of agent-based and Cloud Computing for the smart objects-oriented IoT. Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD).doi:10.1109/cscwd.2014.6846894

[8] Vaquero, L. M., & Rodero-Merino, L. (2014). Finding your Way in the Fog. ACM SIGCOMM Computer Communication Review, 44(5), 27–32. doi:10.1145/2677046.2677052

[10] C. H. Hong, B. Varghese, "Resource Management in Fog/Edge Computing: A Survey," arXiv:1810.00305v1 [cs.DC] 30 Sep 2018.

[11] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing - MCC '12.doi:10.1145/2342509.2342513

[12] Feng Tian. (2017). A supply chain traceability system for food safety based on HACCP, Blockchain & Internet of things. 2017 International Conference on Service Systems and Service Management.doi:10.1109/icsssm.2017.7996119

[13] https://coinmarketcap.com/fr/currencies/bitcoin/

[14] Satoshi Nakamoto https://bitcoin.org/bitcoin.pdf

[15] Atzori, M. (2015). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? SSRN Electronic Journal. doi:10.2139/ssrn.2709713

[16] Biswas, K., & Muthukkumarasamy, V. (2016). Securing Smart Cities Using Blockchain Technology. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). doi:10.1109/hpcc-smartcity-dss.2016.0198

[17] Certicom Research. "SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0." January 27, 2010. Document http://www.secg.org/sec2-v2.pdf

[18] Sánchez de Pedro Crespo, Adán & Ivan Cuende García, Luis. (2017). Blockchain Timestamping Architecture Version 6 (BTAv6). doi: 10.13140/RG.2.2.17223.80805.

[19] Sinclair Davidson, Primavera de Filippi, Jason Potts. Economics of Blockchain. Public Choice Conference, May 2016, Fort Lauderdale, United States. doi : 10.2139/ssrn.2744751

[20] N. Szabo, "Smart Contracts," 1994. http://szabo.best.vwh.net/smart.contracts.html and http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[21] Jani, Shailak. (2018). "An Overview of Ethereum & Its Comparison with Bitcoin", International Journal of Scientific & Engineering Research

-[22] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, 2017 "Lsb: A lightweight scalable Blockchain for IoT security and privacy," arXiv preprint arXiv:1712.02969

[23] Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal, 5(2), 1184–1195. doi:10.1109/jIoT.2018.2812239

[24] Liang, X., Zhao, J., Shetty, S., & Li, D. (2017). Towards data assurance and resilience in IoT using Blockchain. MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM). doi:10.1109/milcom.2017.8170858

[25] Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards Blockchain-based Auditable Storage and Sharing of IoT Data. Proceedings of the 2017 on Cloud Computing Security Workshop - CCSW '17. doi:10.1145/3140649.3140656

[26] Cebe, M., Erdin, E., Akkaya, K., Aksu, H., & Uluagac, S. (2018). Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. IEEE Communications Magazine, 56(10), 50–57. doi:10.1109/mcom.2018.1800137

[27] Lin, J., Shen, Z., & Miao, C. (2017). Using Blockchain Technology to Build Trust in Sharing LoRaWAN IoT. Proceedings of the 2nd International Conference on Crowd Science and Engineering - ICCSE'17. doi:10.1145/3126973.3126980